法务、合规、内控、风险一体化管理原则与实施指南

1 范围

本文件规定企业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。

本文件可帮助企业实现对其法务管理、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。这些整合将为企业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。

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企业的整合管理体系中且全部得到满足，企业才能声明符合本文件。

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

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

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

注：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：管理体系的范围可能包括整个企业、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 **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。

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企业(3.1.2)的一个人或一组人。

注：最高管理者有权在企业内部授权并提供资源。

注：若管理体系(3.1.1)的范围仅覆盖企业的一部分，则最高管理者是指那些指挥并控制企业该部分的人员。

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企业(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

对企业（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（3.1.3）向其报告并对其负责。

注：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：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，以实现企业目标的一项措施。

3.2 与策划有关的术语

3.2.1 **内控** internal control

企业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：影响指对预期的偏离----正面的或负面的。

注：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(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）企业(3.1.2)必须遵守的法律法规要求(3.2.5)，以及企业必须遵守或选择遵守的其他要求。

注：合规义务是与合规管理体系(3.1.1)相关的。

注：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、通常隐含的或必须满足的需求或期望。

注：“通常隐含的”是指对企业(3.1.2)和相关方(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：法律法规要求以外的要求一经企业决定遵守即成为义务。

3.2.6 目标 objective

要实现的结果。

注：目标可能是战略性的、战术性的或运行层面的。

注：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、企业层面的、项目、产品、服务和过程(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

企业(3.1.2)需要控制并保持的信息，以及承载信息的载体。

注：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：文件化信息可能涉及：

——为企业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）。

3.3.3 外包 outsource

安排外部企业(3.1.2)承担企业的部分职能或过程(3.3.4)。

注：虽然外包的职能或过程是在企业的管理体系(3.1.1)覆盖范围内，但是外部企业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(3.3.4)。

注：内部审核由企业(3.1.2)自行实施执行或由外部其他方代表其实施。

注：审核可以是结合审核（结合两个或多个领域）。

注：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(3.2.5)。

3.4.3 不符合 nonconformity

未满足要求(3.2.5)。

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

3.4.4 纠正措施 corrective action

为消除不符合(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(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(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(3.3.4)。

3.4.9 绩效 performance

可度量的结果。

注：绩效可能与定量或定性的发现有关。

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

4 企业环境

4.1 理解企业及其环境

企业应确定与其宗旨、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。这些因素应包括受企业影响的或能够影响企业的内外环境状况。

企业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：这些因素可能包括需要考虑的正面和负面条件。

注：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;考虑与企业的价值观、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

企业应明确：

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

企业应确定法务、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。

确定范围时企业应考虑：

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

注：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，企业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 企业建立并保持法务、合规、内控、风险一体化管理体系时，应考虑在 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 企业应确定法务、合规、内控、风险一体化管理体系所需的过程及其在整个企业的应用，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，并确保其与企业的战略方向相一致；

c） 确保将法务、合规、内控、风险一体化管理要求融入企业的业务过程；

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企业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。企业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企业层面的领导分管，或者建立部门层面的联席会议机制；

c） 岗位职责一体化。企业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） 企业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） 适合于企业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

企业法务、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) 在企业内得到沟通；

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企业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) 可获得企业法务、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

企业应建立、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，企业应考虑：

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。

企业应确定其法务、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。

企业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。

—— 企业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

企业应：

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企业；

企业应保持其合规义务、内控规范与风险准则的文件化信息。

6.1.3 措施的策划

企业应策划：

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，企业应考虑其可选技术、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 企业应针对其相关职能，建立法务、合规、内控、风险一体化管理目标。

企业法务、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。

企业应保持法务、合规、内控、风险一体化管理目标的文件化信息。

6.2.2 企业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。

企业法务、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，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，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）。

企业应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

当企业确定需要对法务、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）

企业应考虑：

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

企业应确定并提供建立、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

企业应：

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。

企业应保留适当的文件化信息作为能力的证据。

7.3 意识

企业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) 对企业法务、合规、内控、风险一体化管理有效性的贡献；

a) 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

企业应建立、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，企业应：

——必须考虑其法务、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。

企业应对其法务、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，企业应保留文件化信息，作为其信息交流的证据。

7.4.2 信息沟通

企业应：

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) 在企业各职能就法务、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；