



中华人民共和国国家标准

GB/T 35770—2022/ISO 37301:2021

代替 GB/T 35770—2017

合规管理体系 要求及使用指南

Compliance management systems—Requirements with guidance for use

(ISO 37301:2021, IDT)

2022-10-12 发布

2022-10-12 实施



国家市场监督管理总局 发布
国家标准化管理委员会

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 组织环境 4

 4.1 理解组织及其环境 4

 4.2 理解相关方的需要和期望 5

 4.3 确定合规管理体系的范围 5

 4.4 合规管理体系 5

 4.5 合规义务 5

 4.6 合规风险评估 5

5 领导作用 6

 5.1 领导作用和承诺 6

 5.2 合规方针 6

 5.3 岗位、职责和权限 7

6 策划 8

 6.1 应对风险和机会的措施 8

 6.2 合规目标及其实现的策划 9

 6.3 针对变更的策划 9

7 支持 9

 7.1 资源 9

 7.2 能力 10

 7.3 意识 10

 7.4 沟通 11

 7.5 文件化信息 11

8 运行 12

 8.1 运行的策划和控制 12

 8.2 确立控制和程序 12

 8.3 提出疑虑 12

 8.4 调查过程 12

9 绩效评价 13

 9.1 监视、测量、分析和评价 13

9.2 内部审核 14

9.3 管理评审 14

10 改进 15

10.1 持续改进 15

10.2 不符合与纠正措施 15

附录 A（资料性） 本文件使用指南 16

附录 NA（资料性） 补充使用指南 32

参考文献 36

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。

本文件代替 GB/T 35770—2017《合规管理体系 指南》，与 GB/T 35770—2017 相比，除结构调整和编辑性改动外，主要技术变化如下：

- 更改了文件类型，由指南类管理体系标准修改为要求类管理体系标准；
- 修改了方针、过程、要求、合格、不合格、纠正措施、审核、测量、监视、治理机构、合规风险、合规义务、合规、不合规、程序的术语和定义（见 3.5、3.8、3.14、3.15、3.16、3.17、3.18、3.19、3.20、3.21、3.24、3.25、3.26、3.27、3.31，2017 年版的 2.8、2.10、2.13、2.32、2.33、2.35、2.31、2.30、2.29、2.4、2.12、2.16、2.17、2.18、2.25）。

本文件等同采用 ISO 37301:2021《合规管理体系 要求及使用指南》。与 ISO 37301:2021 相比，本文件做了下列最小限度的编辑性改动：

- 术语 3.14 增加了注，对要求做了进一步解释；
- 术语 3.28 增加了注，对组织价值观进行了解释；
- 考虑到本文件在我国的适用性，增加了附录 NA（资料性）。

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。

本文件由中国标准化研究院提出并归口。

本文件起草单位：中国标准化研究院、北京大成律师事务所、中国石油天然气集团有限公司、中标合信(北京)认证有限公司、中建科技集团有限公司、北京在礼合规信息技术有限公司、北京大成(上海)律师事务所、中国工商银行股份有限公司、中国质量认证中心、通标标准技术服务有限公司、中国信息通信研究院、北京康柏汉森医药科技咨询有限责任公司、北京申永企业管理咨询有限公司、上海段和段律师事务所、山东鲁源节能认证技术工程有限公司。

本文件主要起草人：王益谊、杜晓燕、徐永前、吴学静、蒋汉才、李近宇、王耕杰、王超、张利宾、李铁男、胡国辉、陈立彤、樊光中、牛娜娜、张怡、王培勋、辛斌、李文宇、刘翠东、任建芝、刘红霞、卢博宇、姚竹新、吕菊萍、张波、温利峰、张大春、尹云霞、逢华。

本文件所代替文件的历次版本发布情况为：

- 2017 年首次发布为 GB/T 35770—2017；
- 本次为第一次修订。

引言

为获得长远发展,组织需基于相关方的需要和期望确立并维护合规文化。因此,合规是实现组织成功和持续发展的基石和机会。

合规是一个持续的过程,也是组织履行其义务的结果。合规的可持续性体现在将合规融入组织文化以及为组织工作的人的行为和意识。合规管理在保持独立性的同时,最好与组织的其他管理过程、运行需求和程序相结合。

一个全面有效的合规管理体系,能证实组织承诺并致力于遵守相关法律、监管要求、行业准则和组织标准,以及良好治理标准、普遍接受的最佳实践、道德规范和社区期望。

组织的领导层运用核心价值观、普遍接受的良好治理方法、道德规范和社会准则来塑造组织的合规之道。将合规融入为组织工作的人员的行为取决于组织各层级的领导作用、组织的清晰价值观以及组织对促进合规行为措施的认可和实施。如果组织的各层级不能做到上述各点,则面临不合规的风险。在许多司法管辖区,法院在对违反相关法律的行为做出适当处罚的决定时,根据组织的合规管理体系考虑了其合规承诺。因此,监管部门和司法机构也能利用本文件对标而受益。

通过推行具有约束力的价值观和实施适当的合规管理,组织将更加确信其可以有效维护自身诚信,避免或尽量减少违反组织的合规义务。因此,诚信和有效合规是组织实现良好勤勉管理的关键要素。合规还有助于组织履行社会责任。

本文件的目标之一是协助组织开发和传播积极的合规文化。建议组织将合规相关风险的有效及合规管理视为可追求和利用的机会,因其为组织提供下列优势:

- 增加业务机会、促进可持续发展;
- 保护并提升组织的声誉和信誉;
- 考虑各相关方的期望;
- 证实组织切实有效管理其合规风险的承诺;
- 提升第三方对组织取得持续成功的信心;
- 最大限度地降低违规行为导致的风险及相应的成本和声誉损失。

本文件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。本文件中的要求与指南旨在具有适应性,根据组织合规管理体系规模和成熟度的不同,以及组织活动和目标所处的环境、性质及其复杂程度的不同,其实施方式有所不同。

本文件适用于加强其他管理体系的合规相关要求的履行,有助于提升组织对所有合规义务的统筹管理。

图1概述了合规管理体系的常见要件。

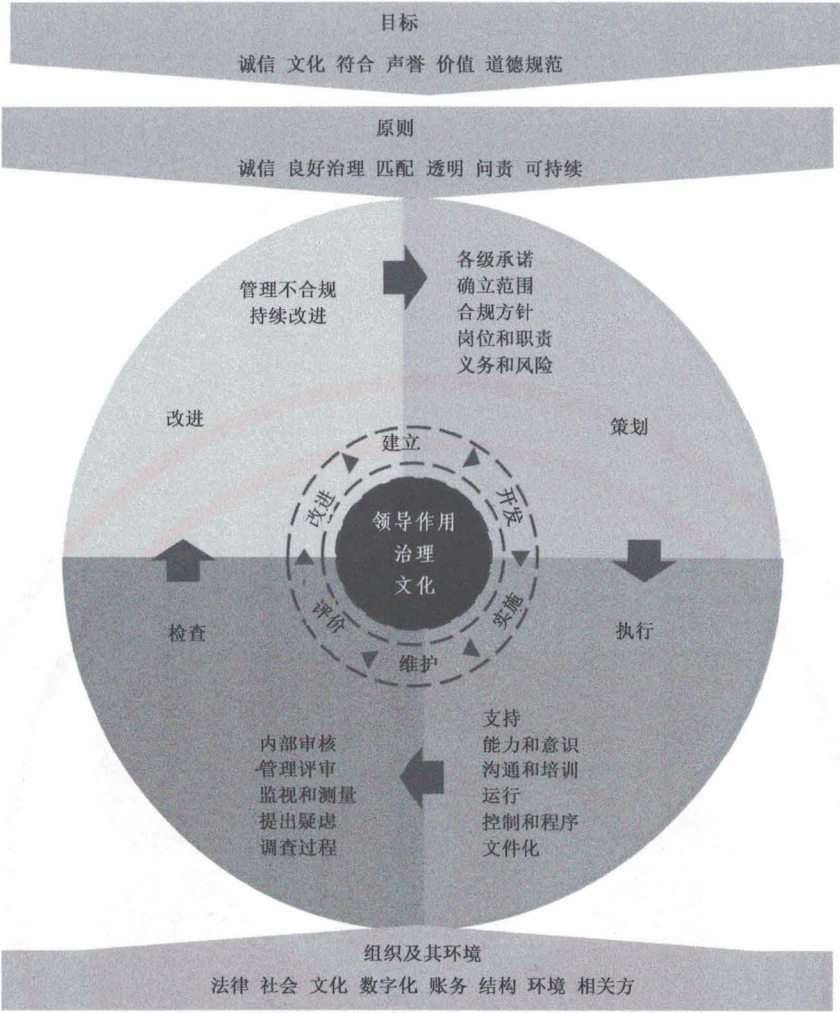


图 1 合规管理体系要件

本文件使用如下能愿动词：

- “应”表示要求；
- “宜”表示推荐；
- “可”表示允许；
- “能”表示能力或可能性。

本文件“注”的信息是理解或说明相关要求的指南。

附录 A 提供了本文件的使用指南，附录 NA 提供了本文件的补充使用指南。

合规管理体系 要求及使用指南

1 范围

本文件规定了组织建立、开发、实施、评价、维护和改进有效的合规管理体系的要求,并提供了指南。本文件适用于所有类型的组织,不论其类型、规模、性质,也不论其是公共的、私营的或非营利性的。如果组织内没有设立独立的治理机构,则本文件中规定的所有关于治理机构的要求都适用于最高管理者。

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

组织 organization

为实现目标(3.6),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1:组织的概念包括但不限于个体经营者、公司、集团公司、商行,企事业单位、行政机构、合伙企业、慈善机构或研究机构,或上述组织的部分或组合,无论是否具有法人资格,公有或私有。

注2:如果组织是大型实体的某个组成部分,那么,术语“组织”仅指在合规管理体系(3.4)范围内的这个组成部分。

3.2

相关方 interested party(优先术语)

利益相关方 stakeholder(许用术语)

能够影响决策或活动、受决策或活动影响或自认为受决策或活动影响的个人或组织(3.1)。

3.3

最高管理者 top management

在最高层指挥和控制组织(3.1)的一个人或一组人。

注1:最高管理者有权在组织内部授权和提供资源。

注2:如果管理体系(3.4)的范围仅覆盖组织的某个组成部分,那么最高管理者是指挥和控制该部分的一个人或一组人。

注3:本文件中,“最高管理者”指最高级别的执行管理层。

3.4

管理体系 management system

组织(3.1)为确立方针(3.5)和目标(3.6)以及实现这些目标的过程(3.8)所形成的相互关联或相互作用的一组要件。

注1:一个管理体系可能针对一个或几个主题。

注2:管理体系要件包括组织的结构、岗位和职责、策划和运行。

3.5

方针 policy

由最高管理者(3.3)正式表述的组织(3.1)的意图和方向。

注：方针也可能由组织的治理机构(3.21)正式表述。

3.6

目标 objective

要实现的结果。

注 1：目标可能是战略的、战术的或运行的。

注 2：目标可能涉及不同的主题(如财务、健康和安全、环境)。它们可能存在于不同层面,诸如组织整体层面或项目、产品、服务或过程(3.8)层面。

注 3：目标能够用其他方式表述,如:预期的结果、宗旨、运行准则,合规(3.26)目标或使用其他有类似含义的词(如:终点或指标)。

注 4：在合规管理体系(3.4)中,组织(3.1)设定的合规目标与合规方针(3.5)保持一致,以实现特定的结果。

3.7

风险 risk

不确定性对目标(3.6)的影响。

注 1：影响是对预期的偏离——正面的或负面的。

注 2：不确定性是一种状态,是指对某个事件、事件的后果或可能性缺乏甚至部分缺乏相关信息、理解或知识。

注 3：通常,风险以潜在事件(见 ISO Guide 73 的定义)和后果(见 ISO Guide 73 的定义)或二者的组合来描述其特性。

注 4：通常,风险以某个事件的后果(包括情况的变化)及其发生的可能性(见 ISO Guide 73 的定义)的组合来表述。

3.8

过程 process

使用或转化输入以实现结果的一组相互关联或相互作用的活动。

注：某个过程的结果是称为输出,还是称为产品或服务,取决于相关语境。

3.9

能力 competence

应用知识和技能实现预期结果的本领。

3.10

文件化信息 documented information

组织(3.1)需要控制和维护的信息及其载体。

注 1：文件化信息能够以任何形式和载体存在,且来源不限。

注 2：文件化信息可能涉及：

——管理体系(3.4),包括相关过程(3.8);

——为组织运行而创建的信息(文件);

——实现的结果的证据(记录)。

3.11

绩效 performance

可测量的结果。

注 1：绩效可能涉及定量的或定性的结果。

注 2：绩效可能与活动、过程(3.8)、产品、服务、体系或组织(3.1)的管理有关。

3.12

持续改进 continual improvement

提高绩效(3.11)的循环活动。

3.13

有效性 effectiveness

完成策划的活动和实现策划的结果的程度。

3.14

要求/需求 requirement

规定的、不言而喻的或有义务履行的需要或期望。

注 1：不言而喻的或有义务履行的需要或期望是指需求。其中，“不言而喻”是指组织(3.1)和相关方(3.2)的惯例或一般做法，不言而喻的需要或期望是不用说就明白的。

注 2：规定的需要或期望是指要求，也就是符合 GB/T 1.1—2020 中定义的要求，即表达声明符合该文件需要满足的客观可证实的准则。

注 3：规定的需要或期望是指要求，例如文件化信息(3.10)中。

3.15

符合 conformity

满足要求(3.14)。

3.16

不符合 nonconformity

未满足要求(3.14)。

注：不符合不一定是违规(3.27)。

3.17

纠正措施 corrective action

为了消除不符合(3.16)的原因并预防再次发生所采取的措施。

3.18

审核 audit

获取审核证据并对其进行客观评价，以确定审核准则满足程度所进行的系统的、独立的过程(3.8)。

注 1：审核可能为内部(第一方)审核或外部[第二方或第三方(3.30)]审核，也可能为多体系审核(合并两个或多个主题)。

注 2：内部审核由组织(3.1)自行实施或代表组织的外部机构实施。

注 3：“审核证据”和“审核准则”的定义见 ISO 19011。

注 4：独立性能够通过正在被审核的活动免于承担责任或无偏见和利益冲突来证实。

3.19

测量 measurement

确定数值的过程(3.8)。

3.20

监视 monitoring

确定体系、过程(3.8)或活动的状态。

注：确定状态可能需要检查、监督或严格观察。

3.21

治理机构 governing body

对组织(3.1)的活动、治理、方针(3.5)负有最终职责和权限的一个人或一组人，最高管理者(3.3)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。

3.22

人员 personnel

在国家法律或实践中被确认为工作关系的个人,或依赖于组织(3.1)活动的任何合同关系中的个人。

3.23

合规团队 compliance function

对合规(3.26)管理体系(3.4)运行负有职责、享有权限的一个人或一组人。

注:最好指定一人负责合规管理体系的监督。

3.24

合规风险 compliance risk

因未遵守组织(3.1)合规义务(3.25)而发生不合规(3.27)的可能性及其后果。

3.25

合规义务 compliance obligations

组织(3.1)强制性地必须遵守的要求(3.14),以及组织自愿选择遵守的要求。

3.26

合规 compliance

履行组织(3.1)的全部合规义务(3.25)。

3.27

不合规 noncompliance

未履行合规义务(3.25)。

3.28

合规文化 compliance culture

贯穿整个组织(3.1)的价值观、道德规范、信仰和行为(3.29),并与组织结构和控制系统相互作用,产生有利于合规(3.26)的行为规范。

注:价值观是组织所崇尚的文化的核心,是组织行为的基本原则。

3.29

行为 conduct

影响顾客、员工、供应商、市场和社区结果的举动和实践。

3.30

第三方 third party

独立于组织(3.1)的个人或机构。

注:所有业务伙伴都是第三方,但并非所有第三方都是业务伙伴。

3.31

程序 procedure

为进行某项活动或过程(3.8)所规定的途径。

[来源:GB/T 19000—2016,3.4.5]

4 组织环境

4.1 理解组织及其环境

组织应确定与其宗旨相关的,并影响其实现合规管理体系预期结果的能力的内部和外部事项。