ICS 03.100.01
CCS A 02

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
国家标准化管理委员会　发布

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、逄华。

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理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。

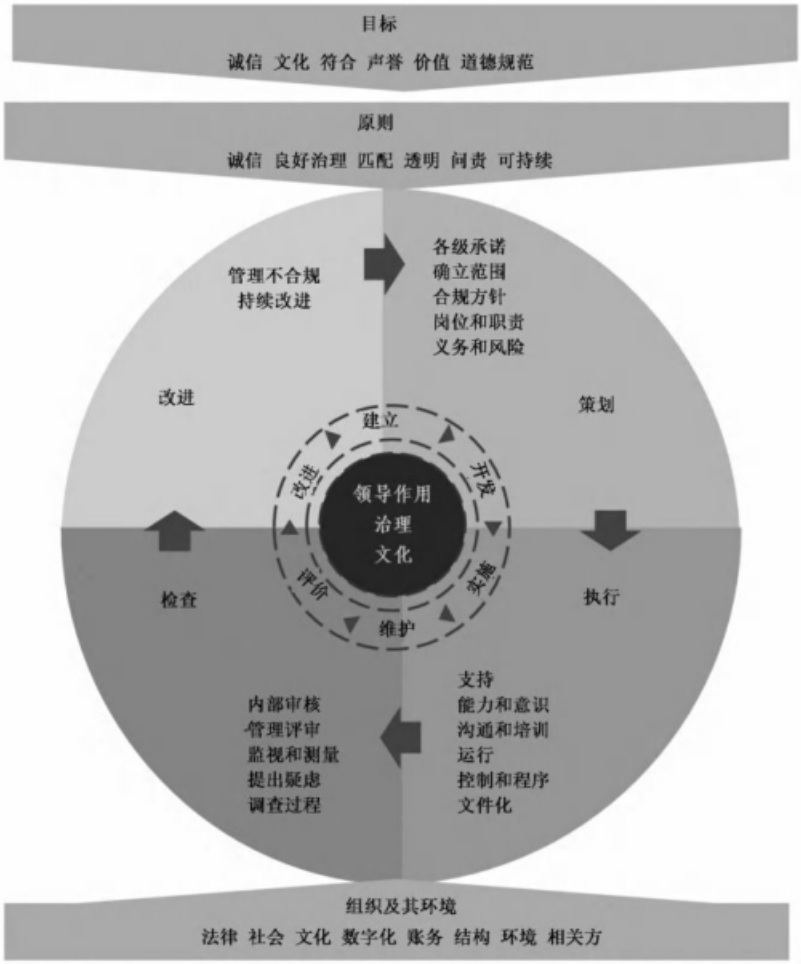

图 1　合规管理体系要件

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：不符合不一定是不合规(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：独立性能通过对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。

为此，组织应结合诸多事项，包括但不限于：

——业务模式，包括组织活动和运行的战略、性质、规模、复杂性和可持续性；

——与第三方业务关系的性质和范围；

——法律和监管环境；

——经济状况；

——社会、文化、环境背景；

——内部结构、方针、过程、程序和资源，包括技术；

——自身的合规文化。

4.2 理解相关方的需要和期望

组织应确定：

——与合规管理体系有关的相关方；

——这些相关方的有关需求；

——哪些需求将通过合规管理体系予以解决。

4.3 确定合规管理体系的范围

组织应确定合规管理体系的边界和适用性，以确立其范围。

注：合规管理体系的范围旨在理清组织面临的主要合规风险，以及合规管理体系适用的地理和/或组织边界，尤其当组织是较大实体的一部分时。

组织应根据以下内容确定合规管理体系的范围：

——4.1 提及的内部和外部事项；

——4.2、4.5 和 4.6 提及的需求。

范围应作为文件化信息可获取。

4.4 合规管理体系

组织根据本文件的要求，应建立、实施、维护和持续改进合规管理体系，包括所需的过程及其相互作用。

合规管理体系应反映组织的价值观、目标、战略和合规风险，并且应结合组织环境（见 4.1）。

4.5 合规义务

组织应系统识别来源于组织活动、产品和服务的合规义务，并评估其对运行所产生的影响。

组织应建立过程以：

a) 识别新增及变更的合规义务，确保持续合规；

b) 评价已识别的变更的义务所产生的影响，并对合规义务管理实施必要的调整。

组织应维护其合规义务的文件化信息。

4.6 合规风险评估

组织应基于合规风险评估，识别、分析和评价其合规风险。

组织应通过将其合规义务与活动、产品、服务以及运行的相关方面关联，来识别合规风险。

组织应评估与外包的和第三方的过程相关的合规风险。

组织应定期评估合规风险，并在组织环境发生重大变化时进行评估。

组织应保留有关合规风险评估和应对合规风险措施的文件化信息。

5 领导作用

5.1 领导作用和承诺

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以下方面证实其对合规管理体系的领导作用和承诺：

——确保合规方针和合规目标得以确立，并与组织的战略方向一致；

——确保将合规管理体系要求融入组织的业务过程；

——确保合规管理体系所需的资源可获取；

——就有效的合规管理的重要性以及符合合规管理体系要求的重要性进行沟通；

——确保合规管理体系实现其预期结果；

——指导和支持人员为合规管理体系的有效性作出贡献；

——促进持续改进；

——支持其他相关岗位在职责范围内证实其领导作用。

注：本文件中提到的"业务"能够广义地理解为涉及组织宗旨的那些核心活动。

治理机构和最高管理者应：

——确立和坚持组织的价值观；

——确保制定并实施方针、过程和程序，以实现合规目标；

——确保能及时获知合规事件，包括不合规情况，并确保采取适当措施；

——确保维护合规承诺，并妥善处理不合规和不合规行为；

——视情况确保合规责任在工作职责说明中得到体现；

——任命或提名合规团队(见 5.3.2)；

——确保根据 8.3 确立了提出和解决疑虑的机制。

5.1.2 合规文化

组织应在其内部各个层级建立、维护并推进合规文化。

治理机构、最高管理者和管理者应证实，对于整个组织所要求的共同行为准则，其做出了积极的、明示的、一致且持续的承诺。

最高管理者应鼓励创建和支持合规的行为，应阻止且不容忍损害合规的行为。

5.1.3 合规治理

治理机构和最高管理者应确保下列原则得到实施：

——合规团队应能直接接触治理机构；

——合规团队的独立性；

——合规团队具有适当的权限和能力。

注 1：直接接触包括：向治理机构的直接汇报线、定期提交报告以及参加其会议。

注 2：独立性是指合规团队的运行不受任何不当干扰和/或压力。

5.2 合规方针

治理机构和最高管理者应确立合规方针，该方针：

a) 适合于组织的宗旨，

b) 为设定合规目标提供框架，

c) 包括满足适用需求的承诺，

d) 包括持续改进合规管理体系的承诺。

合规方针应：

——与组织的价值观、目标和战略保持一致；

——要求遵守组织的合规义务；

——根据 5.1.3 支持合规治理原则；

——提及并描述合规职能；

——概述不遵守组织的合规义务、方针、过程和程序的后果；

——鼓励提出疑虑，并且禁止任何形式的报复；

——用通俗易懂的语言书写，易于所有人员理解其原则和意图；

——被适当地实施和执行；

——作为文件化信息可获取；

——在组织内予以沟通；

——视情况，可被相关方获取。

5.3 岗位、职责和权限

5.3.1 治理机构和最高管理者

治理机构和最高管理者应确保在组织内分配并沟通相关岗位的职责和权限。

治理机构和最高管理者应分配职责和权限，以便：

a) 确保合规管理体系符合本文件的要求；

b) 获得合规管理体系绩效的报告。

治理机构应：

——确保根据合规目标的实现情况对最高管理者进行衡量；

——对最高管理者运行合规管理体系的情况进行监督。

最高管理者应：

——为建立、制定、实施、评价、维护和改进合规管理体系配置足够且适当的资源；

——确保建立及时有效的合规绩效报告制度；

——确保战略和运行目标与合规义务相协同；

——确立和维护问责机制，包括纪律处分和结果；

——确保合规绩效与人员绩效考核挂钩。

5.3.2 合规团队

合规团队应负责合规管理体系的运行，包括：

——推进识别合规义务；

——编制合规风险评估文件(见 4.6)；

——使合规管理体系与合规目标保持一致；

——监视和测量合规绩效；

——分析和评价合规管理体系的绩效，以确认是否需要采取纠正措施；

——确立合规报告和文件化制度；

——确保按策划的时间间隔对合规管理体系进行评审(见 9.2 和 9.3)；

——确立提出疑虑和确保疑虑得到解决的制度。

合规团队应监督：

——履行已识别的合规义务的职责在整个组织内得到适当分配；

——合规义务与方针、过程和程序的整合；

——所有相关人员按要求接受培训；

——确立合规绩效指标。

合规团队应：

——使人员可获得与合规方针、过程和程序有关的资源；

——就合规相关事项向组织提供建议。

注：合规团队的特定职责并不免除其他人员的合规责任。

组织应确保合规团队能接触：

——高级决策者，并有机会在决策早期提出建议；

——组织的所有层级；

——所有人员、文件化信息和所需的数据；

——专家关于相关法律、法规、准则和组织标准提出的建议。

5.3.3 管理者

管理者应通过以下方式对其职责范围内的合规工作负责：

——配合和支持合规团队，并鼓励人员也这么做；

——确保在其控制下的所有人员都遵守组织的合规义务、方针、过程和程序；

——识别其运行中的合规风险并进行沟通；

——在其职责范围内将合规义务融入现有的业务实践和程序；

——参加并协助合规培训活动；

——培养人员的合规意识，指导他们满足培训和能力要求；

——鼓励并支持人员提出合规疑虑，并防止任何形式的报复；

——根据要求积极参与合规相关事件和事项的管理、解决；

——确保一经确认需要采取纠正措施时，适当的纠正措施能得到推荐和实施。

5.3.4 人员

所有人员应：

——遵守组织的合规义务、方针、过程和程序；

——报告合规疑虑、问题和漏洞；

——根据要求参加培训。

6 策划

6.1 应对风险和机会的措施

在策划合规管理体系时，组织应根据4.1提及的事项和4.2提及的需求，并确定需要应对的风险和机会，以便：

——确保合规管理体系能够实现预期结果，

——预防或减少不利影响，

——实现持续改进。

在策划合规管理体系时，组织应结合：

——其合规目标(见 6.2)，

——经识别的合规义务(见 4.5)，

——合规风险评估结果(见 4.6)。

组织应策划以下活动：

a) 应对这些风险和机会的措施；

b) 如何：

1) 将措施纳入合规管理体系过程并实施，

2) 评价这些措施的有效性。

6.2 合规目标及其实现的策划

组织应在相关职能和层级上确立合规目标。

合规目标应：

a) 与合规方针一致；

b) 可测量(如果可行)；

c) 体现适用的需求；

d) 予以监视；

e) 予以沟通；

f) 视情况予以更新；

g) 作为文件化信息可获取。

策划如何实现合规目标时，组织应确定：

——要做什么，

——需要什么资源，

——由谁负责，

——何时完成，

——如何评价结果。

6.3 针对变更的策划

当组织确定需要变更合规管理体系时，应对这些变更的实施进行策划。

组织应结合：

——变更目的及其潜在后果；

——合规管理体系设计和运行的有效性；

——足够的资源的可获取性；

——职责和权限的分配或再分配。

7 支持

7.1 资源

为建立、实施、维护和持续改进合规管理体系，组织应确定并提供所需的资源。

7.2 能力

7.2.1 通则

组织应：

——确定在其控制下工作、影响合规绩效的人员所需的能力；

——确保这些人员在适当的教育、培训或经验的基础上胜任工作；

——适用时，采取措施获得所需的能力，并评价所采取措施的有效性。

适当的文件化信息应作为能力证据可获取。

注：适当的措施可能包括，例如：向现有人员提供培训、指导或重新分配工作；或者聘用或劳务雇用能够胜任的人员。

7.2.2 聘用过程

组织应针对其所有人员开发、确立、实施和维护以下过程：

a) 要求人员遵守组织的合规义务、方针、过程和程序，作为人员的聘用条件；

b) 在聘用后的适当期间内，新聘用人员能获得合规方针的副本或者有渠道获得合规方针，并获得关于合规方针的培训；

c) 对于违反组织合规义务、方针、过程和程序的人员，应采取适当的纪律处分。

作为聘用过程的一部分，组织应结合岗位和人员可能引发的合规风险，在任何聘用、调动和晋升之前按要求进行尽职调查。

组织应实施对绩效目标、绩效奖金和其他激励措施进行定期评审的过程，以验证是否有适当的措施来防止鼓励不合规。

7.2.3 培训

组织应定期对有关人员进行培训，培训应在聘用开始时和组织策划的时间间隔实施。

培训应：

a) 适合于人员的岗位及其面临的合规风险；

b) 进行有效性评估；

c) 进行定期评审。

结合已识别的合规风险，组织应确保实施程序对代表组织开展业务并可能给组织带来合规风险的第三方进行培训，提高其合规意识。

培训记录应作为文件化信息予以保留。

7.3 意识

在组织控制下工作的人员应知道：

——合规方针；

——他们对合规管理体系有效性的贡献，包括改善合规绩效带来的效益；

——不符合合规管理体系要求的后果；

——提出合规疑虑的方法和程序(见 8.3)；

——工作岗位的合规义务与合规方针的关系；

——支持合规文化的重要性。

7.4 沟通

组织应确定与合规管理体系有关的内部和外部沟通，包括：

a) 沟通什么，

b) 何时沟通，

c) 与谁沟通，

d) 如何沟通。

组织应：

——结合沟通需求，综合考虑沟通的多样性和潜在障碍；

——确立沟通的过程，确保结合了相关方的意见；

——在确立沟通过程时：

- 应将其合规文化、合规目标和义务纳入沟通内容；
- 应确保所沟通的合规信息与来源于合规管理体系的信息一致且可信；

——对与合规管理体系相关的沟通内容进行回应；

——视情况，保留文件化信息作为其沟通的证据；

——在组织的各层级和职能内部沟通与合规管理体系有关的信息，视情况包括合规管理体系的变更；

——确保人员能在沟通过程中为合规管理体系的持续改进做出贡献；

——确保人员能在沟通过程中提出合规疑虑(见 8.3)；

——通过组织确立的沟通过程，对外沟通包括其合规文化、合规目标和义务在内的与合规管理体系相关的信息。

7.5 文件化信息

7.5.1 通则

组织的合规管理体系应包括：

a) 本文件要求的文件化信息；

b) 组织确定的，对于合规管理体系有效性所必需的文件化信息。

注：不同组织的合规管理体系文件化信息的程度可能不同，取决于：

——组织的规模及其活动、过程、产品和服务的类型；

——过程及其相互作用的复杂度；

——人员的能力。

7.5.2 文件化信息的创建和更新

在创建和更新文件化信息时，组织应确保适当的：

——标记和说明(例如，标题、日期、作者或文件编号)，

——形式(例如，语言文字、软件版本、图形)和载体(例如，纸质的、电子的)，

——针对适宜性和充分性的评审和批准。

7.5.3 文件化信息的控制

应控制合规管理体系和本文件要求的文件化信息，以确保其：

a) 在需要的场所和时间均可获得并适于使用；

b) 得到充分保护(例如,防止泄密、不当使用或完整性受损)。

为了控制文件化信息,组织应开展以下适用的活动:

——分发、访问、检索和使用;

——存储和防护,包括保持易读性;

——对变更的控制(例如,版本控制);

——保留和处置。

对于组织确定的,策划和运行合规管理体系必要的、来自外部的文件化信息,应视情况进行识别,并予以控制。

注:访问可能意味着只允许查看文件化信息的权限,或者允许并授权查看和变更文件化信息的权限。

8 运行

8.1 运行的策划和控制

为满足要求和实施第6章确定的措施,组织应通过以下方式策划、实施和控制所需的过程:

——对过程确立准则;

——按照准则对过程实施控制。

文件化信息应根据必要程度可获取,以便确认过程已按照策划得到实施。

组织应控制已策划的变更,并评审非预期变更的后果,必要时采取措施减轻不利影响。

组织应确保与合规管理体系相关的,由外部提供的产品、过程或服务受控。

注:对组织运行的外包不会免除组织的法律责任或合规义务。

组织应确保第三方过程得到控制和监视。

8.2 确立控制和程序

组织应实施控制以管理其合规义务和相关合规风险。应对这些控制进行维护、定期评审和测试,以确保其持续有效。

注:测试控制是指实施经过设计的活动以检验控制是否按照既定目的运行,或者不能被规避,或者切实有效地降低风险的后果或可能性。

8.3 提出疑虑

组织应确立、实施并维护一个报告过程,以鼓励和促进(在有合理理由相信信息真实的情况下)报告试图、涉嫌或实际存在的违反合规方针或合规义务的行为。

该过程应:

——在整个组织内可见并可访问;

——对报告保密;

——接受匿名报告;

——保护报告者免于遭受打击报复;

——便于人员获得建议。

组织应确保所有人员了解报告程序、了解其自身的权利和保障机制,并能运用相关程序。

8.4 调查过程

组织应开发、确立、实施并维护过程,以评估、评价、调查有关涉嫌或实际的不合规情形的报告,并做出结论。这些过程应确保能公平、公正的做出决定。

调查过程应由具备相应能力的人员独立进行，且避免利益冲突。

组织应视情况利用调查结果改进合规管理体系(见第10章)。

组织应定期向治理机构或最高管理者报告调查的次数和结果。

组织应保留有关调查的文件化信息。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 通则

组织应对合规管理体系进行监视，以确保实现合规目标。

组织应确定：

——需要监视和测量什么；

——适用的监视、测量、分析和评价的方法，以确保有效的结果；

——何时实施监视和测量；

——何时对监视和测量的结果进行分析和评价。

文件化信息应作为结果证据可获取。

组织应评价合规绩效和合规管理体系的有效性。

9.1.2 合规绩效的反馈来源

组织应确立、实施、评价和维护能够使其从多种渠道寻求并获取合规绩效反馈的过程。组织应对信息进行分析和严格评估，以确认不合规的根本原因，确保采取适当的措施，并在4.6要求的定期风险评估中反映上述信息。

9.1.3 指标的开发

组织应开发、实施和维护一套适当的指标，以帮助组织评价其合规目标的实现情况并评估合规绩效。

9.1.4 合规报告

组织应确立、实施和维护合规报告的过程，以确保：

a) 界定适当的报告准则；

b) 确立定期报告的时间表；

c) 实施非常规报告机制以便于临时报告；

d) 实施保证信息准确性和完整性的机制和过程；

e) 向组织中合适的职能或板块提供准确和完整的信息，以便及时采取预防、纠正和补救措施。

合规团队向治理机构或最高管理者提交的任何报告内容均应受到充分保护，以防止被修改。

9.1.5 记录保存

组织应保留合规活动准确且实时的记录，以协助监视和评审合规过程，并证实其符合合规管理体系要求。

9.2 内部审核

9.2.1 通则

组织应在策划的时间间隔内实施内部审核，以便为合规管理体系提供以下信息：

a) 是否符合：

1) 组织自身对合规管理体系的要求；

2) 本文件的要求。

b) 是否得到了有效地实施和维护。

9.2.2 内部审核方案

组织应策划、确立、实施和维护审核方案，包括频次、方法、职责、策划要求和报告。

组织应根据相关过程的重要性和以往审核的结果，确立内部审核方案。

组织应：

a) 界定每次审核的目标、准则和范围；

b) 选择审核员并实施审核，以确保审核过程的客观性和公正性；

c) 确保向相关管理者和管理层报告审核结果。

注 1：相关管理者可能包括合规团队、最高管理者和治理机构。

文件化信息应作为实施审核方案和审核结果的证据可获取。

注 2：管理体系审核指南见 ISO 19011。

9.3 管理评审

9.3.1 通则

治理机构和最高管理者应在策划的时间间隔内对组织的合规管理体系进行评审，以确保合规管理体系持续的适宜性、充分性和有效性。

9.3.2 管理评审输入

管理评审应包括：

a) 以往管理评审所采取措施的状况；

b) 与合规管理体系有关的外部和内部事项的变化；

c) 与合规管理体系有关的相关方需要和期望的变化；

d) 关于合规绩效的信息，包括以下方面的趋势：

1) 不符合、不合规与纠正措施，

2) 监视和测量的结果，

3) 审核结果；

e) 持续改进的机会。

管理评审应体现：

——合规方针的充分性；

——合规团队的独立性；

——合规目标的达成度；

——资源的充分性；

——合规风险评估的充分性；

——现有控制和绩效指标的有效性；
——与提出疑虑的人员、相关方沟通，包括反馈（见 9.1.2）和投诉；
——调查（见 8.4）；
——报告机制的有效性。

9.3.3 管理评审结果

管理评审的结果应包括持续改进的机会，以及变更合规管理体系的任何需要的决定。
文件化信息应作为管理评审结果证据可获取。

10 改进

10.1 持续改进

组织应持续改进合规管理体系的适宜性、充分性和有效性。

10.2 不符合与纠正措施

发生不符合或不合规时，组织应：
a) 对不符合或不合规做出反应，并且如适用：
   1) 采取控制和纠正措施，
   2) 处置后果；
b) 通过以下活动评价采取措施的需要，以消除产生不符合和/或不合规的原因，避免其再次发生或在其他地方发生：
   1) 评审不符合和/或不合规，
   2) 确定产生不符合和/或不合规的原因，
   3) 确定是否存在或可能发生类似的不符合和/或不合规；
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) 如必要，变更合规管理体系。

纠正措施应与不符合和/或不合规产生的影响相适应。
文件化信息应作为以下事项的证据可获取：
——不符合和/或不合规的性质和所采取的任何后续措施；
——任何纠正措施的结果。

附 录 A
（资料性）
本文件使用指南

A.1 背景和范围

A.1.1 概述

本文件使用指南的目的是指明组织在实施合规管理体系时能采用的方法和措施类型。本指南不是全面性或规范性文件，组织建立符合本文件要求的合规管理体系也没有义务实施本指南中的所有建议。组织宜就其所面临的合规风险的性质和程度采取合理步骤，以履行其合规义务。

组织能够选择将合规管理体系作为一个单独的体系来实施，但理想情况是将其与其他管理体系一起实施，例如风险、反贿赂、质量、环境、信息安全和社会责任等。对此，组织能参考 ISO 31000、ISO 37001、ISO 19001、ISO 14001、ISO/IEC 27001 及 ISO 26000。

A.1.2 范围

任何规模、复杂度或产业的组织都能应用本文件，通过遵守其要求创建合规管理体系。这将便于组织理解其环境、业务运行、由此产生的义务和合规风险，并帮助他们实施合理的步骤来履行义务。本文件正文中的每项要求都需要被遵守。但本附录的指南仅为建议。

在实践中，小型组织通常更容易根据本文件实施合规管理体系，因为它们没有那么复杂。中小型组织通过使用本文件中要求的原则增强其组织的合规实践。

本文件提到了治理机构和最高管理者，并界定了这两个术语在各种语境和位置中的含义。本文件能供所有组织使用，因此如果某个特定组织没有使用这两个术语，那么请留意这两个术语的使用意图：本文件中的要求或指导将适用于在该组织最高层拥有该职责和权限的一个人或一组人。

A.2 规范性引用文件

本文件无规范性引用文件。使用者能参考参考文献了解其他信息以及与合规相关的国际标准。

A.3 术语和定义

本文件采用了 ISO 开发的高层结构（HLS）[1]，以提高其管理体系国际标准之间的一致性。HLS 设定了组成 ISO 管理体系标准（MSS）核心的章条顺序、共用术语和定义以及相同的核心条款。这意味着，一些定义能以不熟悉的方式使用。所提供的定义能在使用本文件时给予澄清说明。

MSS 的这种共用方法增加了此类标准对使用者的价值。它对于选择运行一个（有时称为“融合”）管理体系的组织特别有用，该体系能同时满足两个或多个 MSS 的要求。没有采用 MSS 或合规管理框架的组织能很容易地采用本文件作为其组织内的独立指南。

有关 MSS 和核心内容的更多信息，请访问：https://www.iso.org/management-system-standards.html。

1） 2021 年发布的“ISO/IEC 导则，第 1 部分，2021，《ISO 综合补充件 ISO 专用程序》”中已经将“高层结构”修改为“协调结构”。

A.4 组织环境

A.4.1 理解组织及其环境

本条的目的是协助组织对可能影响其合规管理体系的重要事项确立高层次(例如:战略性)的理解。所获得的知识将用于指导合规管理体系的策划、实施、运行和改进。

这是评审组织所有可获得信息的过程,这些信息包括:该组织做什么、在哪里做、如何以及为什么做。外部以及关键因素将基于它们对组织在合规义务方面产生的影响被予以评估。

最明确的合规义务来源于组织运行的法律和监管环境,而义务或风险也可能来源于本文件中提及的其他因素。组织还宜结合可能产生影响的相关未来趋势。

宜结合内部因素。本文件中列举了一些示例。列表并不详尽,可能还有其他与组织相关的因素。

A.4.2 理解相关方的需要和期望

组织宜对可能影响合规管理体系、受合规管理体系影响或自认为受合规管理体系影响的人或组织的需要和期望确立理解。

有些需要和期望是强制性的,因为它们已被纳入正式要求,如法律、法规、许可、执照以及政府或法院措施。此外还可能有其他未包含的正式要求。

当明确指出相关方的其他需要和期望,并且组织决定将通过签订协议或合同的形式自愿采纳的情况下,这些需要和期望就会成为义务。一旦组织决定采纳,这些需要和期望就会成为合规义务。

外部相关方的示例有:

——政府和政府机构;

——监管机构;

——客户;

——承包商;

——供应商;

——第三方中介机构;

——所有者、股东、投资者;

——非政府组织;

——社会和社区团体;

——业务伙伴。

内部相关方的示例有:

——治理机构;

——管理层;

——员工;

——内部职能,诸如风险管理、内部控制、内部审核、人力资源等。

A.4.3 确定合规管理体系的范围

确定合规管理体系的范围就是组织确立其合规管理体系所适用的物理边界和组织边界。在这个过程中,组织选择在整个组织、组织内特定单元或特定职能内部实施合规管理体系时,具有自由度和灵活性。

通常情况下,合规管理体系会在整个组织中实施,如果组织由多个组织组成,合规管理体系会在所有组织中实施,这样做的目的是为了避免在道德操守和合规方面的双重标准。

合规管理体系的范围宜合理且与组织相匹配，宜考虑组织所面临的合规风险的性质和程度。

确立合规管理体系的范围和确定组织将采纳哪些需求时，宜结合对组织环境的理解和有关的相关方的需求。

A.4.4 合规管理体系

合规管理体系是一个框架，该框架是基本结构、方针、过程和程序的有机组合，其目的是实现预期的合规结果，并发挥作用以预防、发现和响应不合规。

通常，合规管理体系框架具有结构性特征：在必要的基础上构建这个体系。该体系需要通过方针、过程和程序的实施来使其运行，且对其进行维护和持续改进。

合规管理体系包含诸多要件。其中某些要件是为满足预期行为而设计，某些要件用于防止非预期行为而设计，而某些要件用于监视组织的合规绩效或在发生不合规时提出警告。

合规管理体系无法完全避免错误的发生，但有相应的过程确保对错误做出适当的反应，包括对过程、体系和受影响方的补救。

合规管理体系宜以良好治理、匹配性、诚信、透明、问责制和可持续性等原则为基础。

合规管理体系宜作为文件化信息提供。

A.4.5 合规义务

组织宜将合规义务作为建立、开发、实施、评价、维护和改进其合规管理体系的基础。

组织强制遵守的要求能包括：

——法律法规；

——许可、执照或其他形式的授权；

——监管机构发布的命令、条例或指南；

——法院判决或行政决定；

——条约、公约和协议。

组织自愿选择遵守的要求能包括：

——与社会团体或非政府组织签订的协议；

——与公共权力机构和客户签订的协议；

——组织的要求，如方针和程序；

——自愿的原则或规程；

——自愿性标志或环境承诺；

——与组织签署合同产生的义务；

——相关组织的和产业的标准。

组织宜按部门、职能和不同类型的组织性活动来识别合规义务，以便确定谁受到这些合规义务的影响。

获取关于法律和其他合规义务变更信息的过程能包括：

——列入相关监管部门收件人名单；

——成为专业团体的会员；

——订阅相关信息服务；

——参加行业论坛和研讨会；

——监视监管部门网站；

——与监管部门会晤；

——与法律顾问洽商；

——监视合规义务来源(如监管声明和法院判决)。

组织宜采取基于风险的方法，即组织宜首先识别出与业务相关的最重要的合规义务，然后关注所有其他合规义务(帕累托原则)。

适宜时，组织宜确立并维护一个单独文件(如登记册或日志)，列出其所有合规义务，并确立定期更新该文件的过程。

除列出合规义务外，该文件还宜包括但不限于：

——合规义务的影响；

——合规义务的管理；

——与合规义务相关的控制；

——风险评估。

A.4.6 合规风险评估

合规风险评估构成了合规管理体系实施的基础，也是分配适当和充足的资源和过程，以便对已识别的合规风险进行管理的基础。

合规风险能够以不遵守组织的合规方针与义务的后果和不合规发生的可能性来表征。

合规风险包括固有合规风险和剩余合规风险。固有合规风险是指组织在未采取任何相应合规风险处理措施的非受控状态下所面临的全部合规风险。剩余合规风险是指组织现有的合规风险处理措施无法有效控制的合规风险。

组织宜结合不合规的根本原因、来源、后果及其发生的可能性，来分析合规风险。后果可能包括，例如个人和环境伤害、经济损失、名誉损失、行政管理变更以及民事和刑事责任。

合规风险识别包括合规风险源的识别和合规风险情况的界定。组织宜根据部门职责、岗位职责和不同类型的组织活动，识别各部门、职能和不同类型的组织活动中的合规风险源。组织宜定期识别合规风险源，并界定每个合规风险源对应的合规风险情况，开发合规风险源清单和合规风险情况清单。

风险评估涉及将组织能接受的合规风险水平与合规方针中设定的合规风险水平进行比较。

发生下列情形时，宜对合规风险进行周期性再评估：

——新的或变化的活动、产品或服务；

——组织结构或战略变化；

——重大的外部变化，如金融经济环境、市场条件、债务和客户关系；

——合规义务变更；

——并购；

——不合规(即使是单一的不合规事件也能构成情况的实质变化)和近乎不合规。

合规风险评估的详细程度和水平取决于组织的风险情况、环境、规模和目标，并能随着具体的细分领域(如：环境、财务、社会)变化。

基于风险方法的合规管理并不意味着在合规风险较低的情况下组织就接受不合规。它有助于组织集中主要注意力和资源优先处理更高级别风险，最终覆盖所有合规风险。所有已识别的合规风险/情况都会得到监视和处理。

在进行风险评估(相关指导见 ISO 31000)时，宜注意适当的技术(见 IEC 31010)。

A.5 领导作用

A.5.1 领导作用和承诺

A.5.1.1 治理机构和最高管理者

有效的合规要求治理机构和最高管理者的积极承诺，并贯穿于整个组织。

对于合规管理体系而言，治理机构和最高管理者清楚、明确地证实其对实现合规管理体系目标的承诺是至关重要的。

不合规能对业务造成负面影响，如声誉受损、丧失经营许可、丧失机会和巨大成本。因此，治理机构和最高管理者宜认识到有效合规管理的战略重要性。

本文件列出了诸多领导层能证实其承诺的方式。最根本的方式是通过积极和显而易见的支持来建立和维护合规管理体系。

承诺的水平标示为下列事项的实现程度：

——治理机构和所有管理层通过自己的行动和决定，积极证实他们承诺建立、开发、实施、评价、维护和改进的是一个有效且及时响应的合规管理体系；

——合规方针由治理机构正式批准；

——最高管理者对确保组织充分实现关于合规的承诺承担责任；

——所有管理层一致向人员传达一个清晰的信息（通过文字和措施证实）：组织会履行它的合规义务；

——以清晰并令人信服的声明向所有人员和有关的相关方广泛沟通关于合规的承诺，并有措施支持；

——合规团队的员工具有体现有效合规的重要性的适当能力、身份权限和独立性，而且可以直接接触治理机构；

——通过对所有人员和有关的相关方开展意识提升活动和培训，为建立、开发、实施、评价、维护和改进强劲的合规文化提供适当的资源；

——方针、过程和程序不仅反映法律要求，还反映自愿性准则和组织的核心价值观；

——组织向其所有管理层级分配合规责任并要求他们负责；

——定期评审合规管理体系（建议至少每年一次）；

——组织的合规绩效持续改进；

——及时采取纠正措施；

——治理机构和最高管理者遵守组织的合规管理体系。

A.5.1.2 合规文化

支持开发合规文化的因素包括：

——一系列已发布的清晰的价值观；

——管理层积极并显而易见地实施和遵守价值观；

——不论职位，对不合规的一致性处理；

——在指导、辅导和领导中以身作则；

——对潜在的关键职能的人员进行适当的聘用前评估，包括尽职调查；

——在入职培训或新员工训练中强调合规和组织价值观；

——持续进行合规培训，包括更新面向所有人员和有关的相关方的培训；

——持续就合规问题进行沟通；

——绩效考核体系，结合对合规行为的评估，并将合规表现与绩效工资挂钩，以实现合规关键绩效措施和结果；

——对合规管理业绩和结果予以明确认可；

——对故意或因疏忽而违反合规义务的情况给予即时和适当的处分；

——在组织的战略和个人岗位之间建立清晰的联系，强调合规是实现组织结果所必不可少的；

——在内部和外部就合规进行公开和适当的沟通。

合规文化的形成体现于下列方面的实现程度：

——上述事项得以实施；

——相关方（特别是组织的人员）相信上述事项已实施；

——人员理解合规义务与自身活动和所在业务单元活动的相关性；

——组织所有适当层级都按照要求自主应对不合规并采取纠正措施；

——重视合规团队的岗位及其目标；

——人员有能力且受到鼓励向包括最高管理者和治理机构在内的适当的管理层提出合规疑虑。

组织宜：

a) 衡量其合规文化；

b) 寻求所有人员的意见，以确定他们是否感知到治理机构、最高管理者和中层管理者对合规的承诺；

c) 根据组织合规文化指标的结果，确立行动计划。

A.5.1.3 合规治理

合规治理建立在以下基本原则基础上。

合规团队能直接接触治理机构和最高管理者。如有需要，他们能绕过组织中的其他人直接与一个或多个最有权采取行动的人沟通。这直接裨益治理机构和最高管理者，便于他们履行职责。这种接触宜是有计划和系统性的。例如，合规团队能直接向首席执行官报告和间接向审核委员会、主席或整个董事会报告。

合规团队宜是独立的，不与组织结构或其他要件冲突。他们可以自由行动、不受垂直管理者的干涉。

合规团队拥有权限。合规团队在权限上不是一个能被上级否决或被其修改报告或信息的初级部门。合规团队能根据需要指导其他员工。合规团队宜有“发言权”，以申明和提出合规疑虑。

合规团队有足够的资源来支持组织不受限制地执行合规管理体系的必要工作和职责，包括获得技术以使合规管理体系能全面和有效地支持组织实现其合规目标。

A.5.2 合规方针

合规方针确立了组织实现合规的首要原则和行动承诺。它设定了要求的职责和绩效水平，并设定了对行动进行评估的期望。该方针宜与组织活动产生的合规义务相适应。

合规方针宜由治理机构批准。

合规方针宜规定：

——与组织的规模、性质、复杂性及其环境有关的合规管理体系的应用和环境；

——合规与其他职能的结合程度，如与治理、风险、审核和法务；

——对内外部相关方的关系进行管理的原则。

合规方针不宜是一个独立的文件，宜得到其他文件的支持，包括运行方针和过程。

如有必要，宜将合规方针翻译成其他语言。

合规方针宜适合于组织因其范围和活动而产生的合规义务。

开发合规方针，宜结合：

a) 具体的国际、区域或属地义务；

b) 组织的战略、目标、文化和治理方法；

c) 组织结构；

d) 与不合规相关的风险的性质和等级；

e) 采用的标准、准则、内部方针和程序；

f) 行业标准。

合规方针可包括：

——使命宣言；

——总体方针声明；

——管理战略以及责任和资源的分配；

——标准合规程序；

——审核、尽职调查和合规。

A.5.3 岗位、职责和权限

A.5.3.1 治理机构和最高管理者

治理机构的积极参与和监督是有效合规管理体系不可或缺的组成部分。这有助于确保人员充分理解组织的合规方针、合规运行程序以及这些方针和程序如何应用于他们的工作，并确保他们有效地履行合规义务。

为使合规管理体系有效，治理机构和最高管理者需要以身作则，坚持并积极、明确地支持合规与合规管理体系。

许多组织视其规模也有合规管理的全面负责人，尽管该负责人可能有其他岗位或职能，例如现有的委员会、组织的单元或合规专家的外包要件。

最高管理者宜鼓励创造和支持合规的行为，而不宜容忍侵害合规的行为。

最高管理者宜确保：

——组织对合规的承诺与其价值观、目标和战略一致，以便适当地定位合规工作；

——鼓励所有员工承认实现其负责或负有责任的合规目标的重要性；

——创造一种鼓励报告不合规并使报告的员工不会受到报复的环境；

——将合规纳入更广泛的组织文化和文化变更举措中；

——识别不合规并即时采取行动予以纠正或处理；

——运行目标和指标不会影响合规行为。

最高管理者宜参考关键绩效指标和其他关键信息并按策划的时间间隔（例如：每季度或每月）评审合规管理体系的绩效，以确保合规管理体系实现其目标。

合规管理体系的有效性要求最高管理者通过制定标准和实施合理监督做出承诺。最高管理者宜了解合规管理体系的内容和运行，并宜确保组织拥有有效的合规管理体系所需的足够的过程。

A.5.3.2 合规团队

许多组织都由专门人员（例如：合规官）负责日常合规管理，有些组织还设有跨职能合规委员会来协

调整个组织的合规工作。合规团队会与管理层一起合作。

并非所有的组织都创建独立的合规团队；一些组织将此职能分配至现有岗位或职能外包。外包时，组织不宜将全部合规职能分配给第三方。即使组织将部分职能外包，也宜考虑维护组织对这些职能的权限并对其进行监督。

分配合规管理体系职责，宜考虑确保合规团队证实：

——诚信和对合规的承诺；

——有效的沟通和影响力；

——有能力接受建议和指导；

——具备设计、实施和维护合规管理体系的相关能力；

——具备面对测试和挑战的信心、业务知识和经验；

——以战略性、积极的方式对待合规；

——有足够的时间来满足合规岗位的需求。

合规团队宜拥有权限、地位和独立性。权限意味着合规团队被治理机构和最高管理者授予足够的权力。地位意味着其他人员很可能倾听和尊重他/她的意见。独立性意味着合规团队尽可能地不亲自参与可能暴露在合规风险之下的活动。

合规团队履行其岗位不宜存在利益冲突。

A.5.3.3 管理者

最高管理者的职责不宜被视为免除其他各级管理者的合规职责，因为所有管理者都在合规管理体系方面发挥作用。因此，明确设定他们各自的职责并列入其岗位描述之中很重要。

管理者的合规职责必然会根据权限的级别、影响力和其他因素而有所不同，如组织的性质和规模。然而，一些职责很可能在不同的组织中是通用的。

A.5.3.4 人员

所有人员都宜履行合规义务。

人员宜确保了解自己的合规职责并有效地执行这些职责。对此，人员将通过合规管理体系的要件获得支持，如培训、方针和程序以及行为准则。

人员宜积极主动地洞察不足与改进，以促进合规管理体系的绩效。

A.6 策划

A.6.1 风险与机会的应对措施

合规管理体系的策划是在战略层面上开展的，而运行策划则是针对运行层面的策划和控制开展的。

策划的目的是预测可能发生的情况和后果，因此它是预防性的。根据合规风险评估的结果，组织宜策划如何在不利影响发生之前应对它们，以及如何从支持合规管理体系有效性的有利条件或环境中获益。

策划还宜包括确定如何将被认为对合规管理体系必要或有益的行动融入业务活动和过程中。这种融入能通过目标设定、运行控制或其他具体条款(例如：资源规定、能力)实现。还宜策划评价合规管理体系有效性的措施。这包括监视、测量技术、内部审核或管理评审。

A.6.2 合规目标及其实现的策划

目标宜以一种可测量其结果的方式来明确。

合规目标举例：至少每年向相关人员提供合规培训。

宜确定实现目标所需的行动（即“什么”）、相关的时间表（即“何时”）和责任人（即“谁”）。宜根据要求定期监视、记录、评估和更新目标的状态和进度。

A.7 支持

A.7.1 资源

资源包括财务、人力和技术资源，以及获得外部咨询和专业技能的机会、组织基础设施、职业发展情况、技术和关于合规管理与法律义务的同时期参考材料。

A.7.2 能力

A.7.2.1 通则

术语“能力”指运用知识和技能实现预期结果的本领。能力需要知识、经验和技能，以便人员能以有效的方式履行其职能。组织宜为所有人员确定完成其任务所需的专业技能和知识，以便组织能向顾客提供其产品和服务。组织宜确立能力证据（例如：岗位描述、职位说明），以便担任该职位时进行考量。

宜采取措施（例如：培训）以便确保维持现有能力和根据需要获得新的能力。宜有足够的能力证明文件以及为维持或获得这些能力所采取的措施。

A.7.2.2 聘用过程

在聘用或提拔现有人员之前，组织宜进行尽职调查，包括推荐信或者背景调查。

A.7.2.3 培训

治理机构、管理者和负有合规义务的人员宜有能力有效履行其义务。有多种方式可获得能力，包括通过教育、培训或工作经验获得所需的技能和知识。

培训计划的目标是确保人员有能力以符合本组织合规文化和对合规的承诺的方式履行其岗位职责。

经过适当设计和执行的培训能为人员提供一个有效的方式以沟通之前未识别的合规风险。

教育和培训宜：

——在适当的情况下，基于对员工知识和能力差距的评估；

——有足够的灵活性，覆盖了一系列技术，以适应组织和人员的不同需要；

——由经验丰富和有资格的人员进行设计、开发和提供；

——适用时以当地语言提供；

——定期评估和评价其有效性。

如果不合规会造成严重后果，那么互动式培训是最好的培训形式。

组织宜对已发生不当行为的领域进行培训。

当出现下列情况时，宜考虑进行合规再培训：

——职位或职责的变化；

——内部方针、过程和程序的变更；

——组织结构的变化；

——合规义务的变更，特别是法律要求和相关方的需求的变化；

——活动、产品或服务的变化；

——产生于监视、审核、评审、投诉和不合规的问题，包括相关方反馈。

A.7.3 意识

意识涉及确保所有人员都能访问、利用并理解合规方针。

提高合规意识的方法包括但不限于：

——培训(面对面或在线)；

——与最高管理者沟通；

——易于参照执行和容易获得的参考资料；

——定期更新合规问题。

沟通对合规的承诺将：

——建立意识并鼓励人员接受合规管理体系；

——鼓励员工提出有助于持续改进合规绩效的建议。

A.7.4 沟通

宜根据本组织的方针，采取面向所有相关方的务实的对外沟通方式。

相关方包括监管机构、顾客、承包商、供应商、投资者、应急服务机构、非政府组织和周遭人士。

组织宜分配适当的资源和具有相关知识的人以协调和促进与监管的互动。

沟通方式可包括网站和电子邮件、新闻稿、广告和定期通讯、年度(或其他定期)报告、非正式讨论、开放日、焦点小组、社区对话、参与社区活动和热线电话。这些方法能促进理解和接受组织对合规的承诺。

沟通宜坚持透明、适当、可信、响应、可接触和清晰的原则。

A.7.5 文件化信息

A.7.5.1 通则

文件化信息包括：

——组织的合规方针和程序；

——合规管理体系的目标、指标、结构和内容；

——合规岗位和职责的分配；

——相关合规义务的登记册；

——合规风险登记册，并根据合规风险评估过程确定相关措施的优先级；

——不合规、近乎不合规和调查的记录；

——年度合规计划；

——人员记录，包括但不限于培训记录；

——审核过程、审核时间表及相关审核记录。

文件化信息能包括与监管报告要求有关的事项。文件化信息可包括各类媒介(数字的和非数字的)。

A.7.5.2 文件化信息的创建和更新

宜更新文件化信息以反映内部和外部的变化，进而确保它们是现行和最新的。

A.7.5.3 文件化信息的控制

文件化信息能以获取法律建议为目的编制，因此能成为法定豁免权的行使对象。

A.8 运行

A.8.1 运行的策划和控制

一个精心设计的合规管理体系包括各项措施(例如:方针、过程、程序),使得合规文化既有内容又有效果。这些措施应对并旨在减少合规风险评估过程所识别的部分风险。

运行控制的一个基本要件是行为准则,其中规定了本组织对相关合规义务的全面承诺。行为准则宜适用于所有人员并使其能够获得和使用。宜将基于并源自行为准则的合规措施纳入本组织的日常运行,以培育合规文化。

在缺少与业务过程有关的运营控制可能导致偏离合规方针或违反合规义务的情况下,需要对运行进行控制。这些情况可能与所有业务情况、活动或过程(例如:生产、安装、服务、维护)或承包商、供应商或销售商有关。

控制的程度取决于几个因素,如所履行的职能的重要性或复杂性、不合规的潜在后果、相关的或可用的技术支持。

当运行控制失效时,则有必要采取措施来应对一切不期望的结果或影响。

如果组织活动中使用了第三方或外包过程,组织宜对其进行有效的尽职调查,以确保组织对合规的标准和承诺不会降低。第三方的一个例子是产品和服务的提供以及产品的分销。组织宜确保签订适当的服务水平协议(SLAs),以规定服务提供者的合规义务。

一个设计良好的外包过程宜考虑以下几点:

——启动和持续的尽职调查;

——实施适当的控制;

——进行持续的监视;

——对法律/合同协议的适当评审;

——考虑服务水平协议;

——使用基于本文件认证的第三方。

在与第三方订立合同时,组织宜实施控制,以确保其活动的采购、运行、业务和其他非财务方面得到适当管理。根据组织和交易的规模,组织实施的采购、运行、业务和其他非财务控制能降低合规风险。

A.8.2 确立控制和程序

组织需要有效的控制,以确保组织的合规义务得以履行,不合规得以防止、发现和纠正。控制的设计宜足够严格,以促进在特定的组织活动和运行环境中实现合规义务。在可能的情况下,这种控制宜嵌入到组织的正常过程之中。

控制包括:

——清晰、实用且易于遵守的文件化运行方针、过程、程序和工作指示;

——系统和例外报告;

——批准;

——分离不相容的岗位和职责;

——自动化过程;

——年度合规计划;

——人员绩效计划;

——合规评估和审核;

——证实的管理层承诺和模范行为,以及其他促进合规行为的措施;

——就员工的预期行为(标准、价值观、行为准则)进行积极、公开和频繁的沟通。

在开发支持合规管理的程序时,宜考虑:

——将合规义务纳入程序,包括计算机系统、表格、报告系统、合同和其他法律文件;

——与组织中其他评审和控制职能的一致性;

——持续监视和测量;

——评估和报告(包括管理监督),以确保雇员遵守程序;

——识别、报告和上报针对不合规的情况与不合规的风险的具体安排。

A.8.3 提出疑虑

适宜时,宜上报至最高管理者和治理机构,包括相关委员会。

即使当地法规未作要求,组织也宜考虑开发匿名或保密的举报人机制,以便组织的员工和代理方能报告不合规或寻求关于不合规的指导,而不必担心遭到报复。

有关举报管理体系的更多指导,见 ISO 37002。

A.8.4 调查过程

有效的合规管理体系的一个特点是具有功能良好的机制,以便及时、彻底地调查对本组织、其人员或有关第三方不当行为的任何指控或怀疑。这包括组织的响应文件、采取的一切处分或补救措施,以及结合经验教训对合规管理体系的修订。

有效的调查机制能确认不当行为的根源、合规管理体系的漏洞和责任缺失的原因,包括管理者、最高管理者和治理机构之间的责任缺失。缜密的根源分析涉及不合规的程度和普遍性,牵涉的人员的数量和水平,以及严重性、持续时间和频率。

组织宜确保调查是公正和独立的。适当时,组织宜考虑创建独立的委员会来监督调查,并保证调查的完整性和独立性。

组织宜确立关于调查的报告机制,包括报告调查结果的级别。

注:法律有时要求组织报告不合规。在这种情况下,监管机构根据适用的法规或其他商定的方式被告知。

即使法律不要求组织报告不合规,组织也能考虑主动向监管机构披露不合规,以减轻不合规的后果。

A.9 绩效评价

A.9.1 监视、测量、分析和评价

A.9.1.1 通则

监视是为了评估合规管理体系的有效性和组织的合规绩效而收集信息的过程。

合规管理体系的监视通常包括:

——培训的有效性;

——控制的有效性(例如通过抽样测试的结果);

——有效分配履行合规义务的职责;

——合规义务的时效性;

——解决先前识别的合规缺陷的有效性;

——未按计划进行内部合规检查的情况;

——针对合规风险对业务战略进行评审,以便适当更新。

合规绩效监视通常包括:

——不合规和“近乎不合规”(即未造成负面影响的事件);
——未履行合规义务的情况;
——未实现目标的情况;
——合规文化现状;
——确立领先的和滞后的指标。

A.9.1.2 合规绩效的反馈来源

来源包括:
——人员(例如:通过举报工具、求助热线、反馈、意见箱);
——顾客(例如:通过投诉处理系统);
——第三方;
——供应商;
——承包商;
——监管机构;
——过程控制日志和活动记录(包括电子版和纸质版)。

合规绩效反馈包括:
——合规问题;
——不合规和合规疑虑;
——新出现的合规问题;
——持续的监管和组织的变更;
——对合规有效性和绩效的评论。

收集信息的方法多种多样。下面列出的每种方法都与其情况相关,宜注意选择适合组织规模、范围、性质和复杂性的工具。

信息收集包括:
——出现或识别出不合规的特别报告;
——通过热线、投诉和其他反馈渠道(包括举报)获得的信息;
——非正式讨论、研讨会和分组座谈会;
——抽样和诚信试验,如神秘购物;
——感知调查的结果;
——直接观察、正式访谈、设施巡察和检查;
——审核和评审;
——相关方质询、培训需要和培训期间的反馈(特别是员工的反馈)。

宜开发信息的分类、存储和检索系统。

信息管理系统宜同时收集问题和投诉,并允许对与合规有关的问题和投诉进行分类和分析。分析宜结合系统性和重复性的问题,以便纠正或改进,因为这些可能会给组织带来更难识别且重大的合规风险。

信息分类类目包括:
——来源;
——部门;
——不合规描述;
——义务类别;

——指标；

——严重性；

——实际或潜在影响。

A.9.1.3 指标的制定

这一过程宜体现合规风险的评估结果，以确保各指标与组织合规风险特征具有相关性。合规绩效是什么和如何测量的问题在某些方面可能具有挑战性，但仍是证实合规管理体系有效性的重要部分。此外，所需的指标将随着组织的成熟程度，实施新的和修订的方案的时间和程度而变化。

指标包括：

——经过有效培训的员工比例；

——监管机构介入的频率；

——反馈机制的使用(包括用户对那些机制价值的评论)。

反应性指标包括：

——按类型、区域和频率报告的已识别的问题和不合规；

——不合规的后果，包括对经济补偿、罚款和其他处罚、补救成本、声誉或员工时间成本影响的估价；

——报告和采取纠正措施所花费的时间。

预测性指标包括：

——以随着时间推移目标的潜在损失/收益(收入、健康和安全、声誉等)测量的不合规的风险；

——不合规趋势(基于过去趋势的预期合规率)。

A.9.1.4 合规报告

尽管报告系统性和反复出现的问题非常重要，但是如果一次性不合规是重大或故意为之的，也能够予以同等重视。即使一个小缺陷，也能表明当前过程和合规管理体系存在严重不足。如果不及时报告，则可能造成人们认为缺陷不重要并可能导致此类缺陷成为系统性问题。

合规报告宜包括：

——组织按要求向任何监管机构通报的任何事项；

——合规义务变更及其对组织的影响，以及为了履行新义务，拟采取的措施方案；

——对合规绩效的测量，包括不合规和持续改进；

——可能的不合规的数量和详细内容，以及随后对它们的分析；

——采取的纠正措施；

——合规管理体系的有效性、业绩和趋势的信息；

——与监管机构的接触和关系进展；

——审核和监视活动的结果；

——监视行动计划的完整执行，特别是那些源自审核报告或监管要求的行动计划，或两者兼而有之。

合规方针宜推进即时报告超出常规报告时间表范围的重大事件。

A.9.1.5 记录保存

记录保存宜包括对合规问题和声称的不合规以及为解决它们而采取的步骤的记录和分类。

记录宜以确保清晰、容易辨认和检索的方式保存。

记录宜受到保护，以免于被增加、删除、修改、未经授权使用或隐藏。

组织的合规管理体系记录包括：

——合规绩效信息，包括合规报告；

——不合规及纠正措施的详细内容；

——对合规管理体系和采取的措施的评审和审核的结果。

A.9.2 内部审核

审核职能，无论其为内部还是外部的，都宜免于利益冲突并保持独立性，以履行其岗位职责。

关于如何对管理体系进行审核的信息见 ISO 19011。

A.9.3 管理评审

管理评审还宜包括以下方面的建议：

——合规方针以及与它相关的目标、体系、结构和人员所需的变化；

——合规过程的变更，以确保与运行实践和体系有效整合；

——需监视的未来潜在不合规的领域；

——与不合规相关的纠正措施；

——当前合规体系和长期持续改进的目标之间的差距或不足；

——对组织内的示范性合规行为的认可。

宜向治理机构提供管理评审中形成文件的结果和全部建议的副本。

A.10 改进

A.10.1 持续改进

合规管理体系的有效性的特点是它具有持续改进和发展的能力。组织的内部、外部环境以及业务随着时间的推移而变化，其顾客的性质和适用的合规义务也随之变化。

宜通过多种方法对合规管理体系的充分性和有效性进行持续和定期评估，例如评审或内部审核。

组织宜确立措施以评审其合规管理体系，并确保其保持最新状态且适合于其目标。在确定支持持续改进的行动的程度和时间尺度时，组织宜结合其环境、经济因素和其他相关情况。

一些组织对员工进行调查，以衡量合规文化，并评价控制的强度。持续改进的进一步信息来源可以是顾客调查的结果、提出疑虑、定期的监视、定期的审核或管理评审。

组织宜结合此类评估的结果和输出，以确定是否需要或有机会变更合规管理体系。

为了有助于确保保持合规管理体系的完整性及有效性，管理体系各个要件的变更宜体现此类变更对整个管理体系有效性的依赖和影响。当对合规管理体系作出变更时，组织宜考虑这些变更对合规管理体系、运行、资源可用性、合规风险评估、组织的合规义务及其持续改进过程的影响。

A.10.2 不符合与纠正措施

未能预防或检测到一次性不合规，并不一定意味着合规管理体系在预防和检测不合规时缺乏有效性。

分析不符合或不合规的信息能用于：

——评估产品和服务性能；

——改进或重新设计产品和服务；

——变更组织惯例和程序；

——再培训员工；

——重新评估告知相关方的需要；

——对潜在不合规做出早期预警；

——重新设计或评审控制；

——加强通知和上报步骤(内部和外部)；

——沟通有关不合规的事实和组织对不合规的立场。

组织宜确认导致不遵守方针或程序或两者皆不遵守之行为发生的根本原因，并根据所吸取的经验教训更新方针和程序。

附 录 NA
（资料性）
补充使用指南

NA.1 合规义务

NA.1.1 概述

4.5 提及的合规义务在 A.4.5 进行了列举。在我国语境下，有些合规义务需要给予补充和提示，例如在我国，除法律法规外，强制性遵守的要求还包括强制性标准（见 NA.1.4）、检察决定（见 NA.1.3）；而有些合规义务则需要做进一步的解释、细化和区分，例如“法律法规”在我国司法管辖区体现为不同形式（见 NA.1.2）；“法院判决”在我国司法管辖区并不具有判例法法域的“遵循先例”的效力，而最高人民法院的指导性案例和司法解释则对法律在司法运用中提供了非常重要的规范，需要进一步解释、细化和区分（见 NA.1.3）；而组织签署合同所产生的义务既可以成为契约性合规义务，也可通过合同援引外国具有域外效力的法律成为组织宣遵循的合规义务的一部分（见 NA.1.5）。

NA.1.2 法律法规

A.4.5 中提及的“法律法规”在我国司法管辖区内主要体现为如下形式：现行有效的法律、行政法规、地方性法规、自治条例和单行条例。其中，法律有广义、狭义两种理解。广义上，法律泛指上述一切具有法律效力的规范性文件；狭义上，仅指全国人大及其常委会制定的规范性文件。在与法规等一起提及时，指狭义上的法律。综上，法律法规一般是指立法部门和执法部门（包括行政和监管部门）制定的法律规范性文件。

NA.1.3 法院判决、检察决定、指导性案例和司法解释

A.4.5 中提及的“法院判决”在我国语境下需要做出补充解释和说明。在我国，法院的判决只对其涉及的案件当事人具有约束力，对于其他相同或类似的案件没有约束力，仅具有参考价值。在法律法规没有对某个案件涉及的问题做出规定的情况下，法院的判决对于相关方了解司法部门所采取的强制性要求具有很强的现实指导意义。另外，除了法院判决外，我国的检察院会做出检察决定。检察决定在我国也构成强制遵守的合规义务。

在我国法域内，最高人民法院、最高人民检察院会颁布指导性案例、司法解释，这些会构成组织强制遵守的合规义务。最高人民法院颁布的指导性案例虽不具备强制约束力，但会成为法院对某些相同或类似案件进行判决的依据。组织为了解相关法律法规在具体案件适用的标准和边界，也要研究最高人民法院颁布的指导性案例。司法解释是最高人民法院、最高人民检察院为解决审判、检察工作中的“具体应用法律的问题”而依法制定的规范性文件，对司法主体与执法主体具有普遍的约束力，效力所及的任何组织和个人都需要遵守。根据 2019 年修订的《最高人民检察院司法解释工作规定》（高检发办字〔2019〕55 号），司法解释采用解释、规则、规定、批复、决定等形式。根据 2021 年最高人民法院颁布的《关于司法解释工作的规定》（法发〔2021〕20 号），司法解释的形式分为解释、规定、规则、批复和决定五种。

NA.1.4 强制性标准

强制性标准在我国也构成组织强制遵守的合规义务。强制性标准，一经发布、必须执行，如

GB 18384—2020、GB 40554.1—2021、GB 18599—2020 等。

NA.1.5 合同安排所产生的义务

根据 A.4.5，组织自愿选择遵守的要求包括“组织的合同安排产生的义务”。这是一种基于契约形成的“合规义务”，这种合规义务来自组织的合作伙伴通过合同条款提出的合规方面的要求。组织一旦选择与这样的合作伙伴进行交易，该组织就要遵守与这个合作伙伴订立的合同所产生的合规义务。合同安排所产生的义务有两种情形，第一种情形是合同条款中直接列明的各项义务；第二种情形是合同条款中纳入法律、法规、强制性标准等强制性要求，这些要求则成为合规义务。

需要注意的是，我国组织在签署国际业务合同时，宜谨慎识别和控制因纳入外国纳入外国法律、法规（包括技术法规）所带来的合规义务与合规风险。这些外国纳入外国法律、法规（包括技术法规）可能与我国法律法规某些强制性规定相违背。一旦签署含有这样条款的合同，我国组织就需要考虑这些条款所援引和纳入的具有域外效力的外国法律以及基于我国的法律法规产生的合规义务与合规风险。

NA.2 合规文化

NA.2.1 合规文化的价值

合规文化通常由贯穿于整个组织的价值观、道德规范、信仰和行为构成，与组织结构和控制系统相互作用，产生有利于实现组织的使命、愿景和合规目标的一系列行为规范。合规文化反映了组织的治理机构、最高管理者、各级管理层、员工和其他相关方应对合规风险的意识和态度，是合规管理体系不可或缺的重要组成部分。

合规文化的价值在于：

——提供原则性指引，应对合规风险：在制定合规管理体系应对合规风险的同时，组织宜宣贯自己的价值观、道德规范和信仰，并据此建立原则性指引，以员工手册、行为准则或其他形式呈现出来，使得组织内外部人员在具体规定不清、不全没有具体规定或灰色地带的情况下，根据原则性指引，开展活动，及时应对合规风险；

——增强主动合规：良好的合规文化可以正面影响人的行为，提升认同感和主动合规意识；有助于组织/各层级及时发现不合规行为并自主采取补救措施；

——提升合规管理有效性，促进实质性合规：组织通过将支持合规文化发展的因素在合规方针中体现，及与合规管理体系的其他要件共同作用，使得合规文化渗透到组织的各个层级和领域，实现预期合规结果。

NA.2.2 合规文化的建立、维护、推广和实施

建立、维护、推广和实施良好合规文化宜考虑以下方面：

——最高层定调并以身作则；

——管理层推动且言行一致；

——团队内良好的合规氛围；

——同事间、相关方正面影响。

组织宜依赖于最高层和管理层运用价值观、道德规范和信仰等塑造合规文化，并以身作则积极推行；宜形成鼓励合规、不容忍不合规的团队氛围，以及对不合规行为进行一致性处理；鼓励和推动同事以及与相关方间合规价值观的传递和影响。

合规文化宜通过合规管理体系的实施反映出来，组织才能有效应对合规风险，降低不合规发生的可能性，实现合规目标。

NA.3 数字化与合规管理

NA.3.1 概述

宜从组织及其环境(见 A.4.1)和组织相关方的需要和期望(见 A.4.2)的角度去理解数字化与合规管理。

NA.3.2 理解组织及其环境的数字化变革

随着数字技术的应用,传统的业务模式和场景正经历数字化转型,涉及交易的签约、交付和支付完全或很大程度上通过数字化方式完成。消费互联网和产业互联网形成了大型的交易平台。随着交易方式的电子化和数字化,新的交易规范(包括法律和法规以及商业惯例)随之形成,通过立法或其他形式被采纳并运用于经济活动中,例如《中华人民共和国民法典》在合同编里增加了有关电子合同的法律规定,以适应数字经济的发展。数字经济的业务模式和规范的产生,势必产生新的合规义务和合规风险(见 A.4.5),例如美国、欧盟和我国关于数据的法律法规以及各种规范指引,包括平台经济的反垄断指引、数据出境安全评估指南等。

组织宜基于其数字化的业务模式识别合规义务,对合规风险进行评估(见 A.4.6)并策划如何应对合规风险。组织宜重视数字经济下的合规义务。

NA.3.3 在合规管理体系中应用数字技术

组织在建立、开发、实施、评价、维护和改进合规管理体系时,宜合理应用数字技术,提升合规管理体系的有效性。

组织宜对应用数字技术形成的管理工具进行测试、优化和不断升级,以提高这些工具的准确性和适用性,并将其与组织的数字化业务过程相融合。

在合规管理体系中应用数字技术的基础是获得完整准确的数据。在合规风险评估(见 A.4.6)、合规管理体系运行(见 A.8)、合规培训(见 A.7.2.3)、合规绩效评价(见 A.9)以及合规管理体系的持续改进(见 A.10)等方面需要组织对相关数据和信息进行收集、分析,并运用于对组织的合规管理。

数字技术在合规管理体系中的应用可包括但不限于以下方面:

——合规义务和相关案件数据库;

——合规风险数据库(包括组织对以往违规行为的总结报告);

——合规培训系统(包括线上课件、自我考试等过程);

——合同管理和财务系统;

——信息和数据搜索与分析工具(例如对组织外部合规相关领域立法和执法趋势的跟踪和分析、对组织内部过往违规事件进行行为模式及发生原因的分析);

——数据分析和示险看板(例如合同履约率的数据分析和示险看板产品)。

NA.4 管理体系一体化融合

NA.4.1 概述

组织建立合规管理体系往往涉及与既有体系的融合,可涉及合规管理基础工具的融合,即法律、内控、风险管理等,也可涉及管理体系间的一体化融合,即质量管理体系、环境管理体系、职业健康安全管理体系、能源管理体系、信息安全管理体系、资产管理体系、反贿赂管理体系等。

合规管理体系与相关体系的一体化融合,并非简单的体系、规则等要求叠加,宜将合规管理与相关管理体系的核心要求、方法与标准相结合。一体化融合宜借助既有组织结构、职责、制度、过程与信息化

等有效要件，尽量避免诸多要件的重复和多体系独立运行导致的职责交叉、管理低效、管控不利的风险。

NA.4.2 融合的范围、方法与路径

一体化融合的范围可涉及治理原则、组织结构与职责、风险识别方法、制度与过程、运行与保障、评价、监督、持续改善和信息化等。一体化融合的方法宜采取制度对标，即识别所需融合的各个管理体系标准与规则，以融合后的要求为基准对组织开展评价、对标梳理，形成统一的治理要求和体系文件并确保其嵌入组织管理职责、制度及内部业务过程。

组织宜根据自身的治理水平、运行状况、业务特点及行业趋势等，开展内外部评价及一体化融合。确定纳入融合范围的管理模块及管理体系，制定一体化融合的实施计划。

一体化融合的路径一般包括以下方面。

a) 构建一体化管理体系要求

组织宜结合自身管理实践，针对融合需求，收集、整理、汇总各项标准与规则，制定一体化管理体系的原则、目标，以便实施、评价一体化融合工作时有据可依。

b) 实施制度对标

组织宜依据一体化管理体系要求开展制度对标，对内部职能、过程及制度进行对标梳理，以确保融合的管理体系能够全面、准确落实到组织的治理体系与日常经营管理中。

c) 形成一体化管理体系文件

体系文件一般包括三个层次，第一层为纲领性文件（如管理手册），第二层为规章制度（如各层级管理制度、办法），第三层为操作规范（如作业指导书）。组织宜根据以下原则形成一体化管理体系文件，即不同标准中相同的要求进行合并，相近的要求进行融合，差异化要求保持独立，并重点关注融合后的体系文件内容是否满足一体化管理体系要求。

d) 运行一体化管理体系

在运行一体化管理体系过程中，组织宜关注体系运行的有效性、各过程、职能的衔接。宜借助合规数字化运行、监督一体化管理体系并实时反馈体系运行情况，确保满足组织预期的目标。

本文件仅为发挥合规管理工具的先进性、最大限度避免体系交叉重叠带来的弊端和风险隐患，并就推进合规管理体系与相关管理体系一体化融合提出一般性原则和实施路径。组织宜根据自身治理情况、行业属性等内外部环境，开展融合工作。融合工作中宜注重合规管理标准、要件和要求的统领性。

参 考 文 献

[1] 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

[2] GB 18384—2020 电动汽车安全要求

[3] GB 18599—2020 一般工业固体废物贮存和填埋污染控制标准

[4] GB/T 19000—2016 质量管理体系 基础和术语

[5] ISO Guide 73 Risk management—Vocabulary

[6] ISO 9000 Quality management systems—Fundamentals and vocabulary

[7] ISO 9001 Quality management systems—Requirements

[8] ISO 14001 Environmental management systems—Requirements with guidance for use

[9] ISO 19011 Guidelines for auditing management systems

[10] ISO 22000 Food safety management systems—Requirements for any organization in the food chain

[11] ISO 26000 Guidance on social responsibility

[12] ISO 31000 Risk management—Guidelines

[13] ISO 37000 Guidance for the governance of organizations

[14] ISO 37001 Anti-bribery management systems—Requirements with guidance for use

[15] ISO 37002 Whistleblowing management systems—Guidelines

[16] ISO/IEC 27001 Information technology—Security techniques—Information security management systems—Requirements

[17] IEC 31010 Risk management—Risk assessment techniques

[18] 中华人民共和国民法典

[19] 最高人民检察院司法解释工作规定(高检发办字〔2019〕55号)

[20] 关于司法解释工作的规定(法发〔2021〕20号)