ICS 03.080
A 02

中华人民共和国国家标准

GB/T ×××××—××××

合规管理体系　指南

Compliance Management Systems—Guidelines

（ISO 19600:2014 Compliance Management Systems—Guidelines，IDT）

征求意见稿

20170204

××××－××－××发布　　××××－××－××实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准使用翻译法等同采用ISO 19600:2014《合规管理体系　指南》。

本标准做了如下编辑性修改：

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这些专利的责任。

本标准由中国标准化研究院提出并归口。

本标准起草单位：

本标准主要起草人：

引　　言

合规是组织可持续发展的基石。近年来，国际社会和各国政府都致力于建立和维护开放、透明、公平的社会秩序，与此同时我国全面推进依法治国，在这样的背景下，组织越来越多地关注其面临的合规风险以及如何实现合规。合规意味着组织遵守了适用的法律法规及监管规定，也遵守了相关标准、合同、有效治理原则或道德准则。若不合规，组织可能遭受法律制裁、监管处罚、重大财产损失和声誉损失，由此造成的风险，即为合规风险。

组织通过建立有效的合规管理体系，来防范合规风险。组织在对其所面临的合规风险进行识别、分析和评价的基础之上，建立并改进合规管理流程，从而达到对风险进行有效的应对和管控。

指南指出合规文化建设的重要性。合规文化是价值观、道德准则和信仰在整个组织中的存在，并与组织的结构和控制系统相互作用，从而产生导致合规结果的行为规范。组织的合规管理最好由领导层打造，管理层应用组织核心价值观、普遍接受的企业治理理念、道德和标准进行合规管理，建设并完善企业的合规文化，从而使企业的合规管理达到事半功倍的效果。

建立有效的合规管理体系并不能杜绝违规的发生，但是能够降低违规发生的风险。在很多国家或地区，当发生违规时，组织和组织的管理者以组织已经建立并实施了有效的合规管理体系作为减轻、甚至豁免行政、刑事或者民事责任的抗辩，这种抗辩有可能被行政执法机关或司法机关所接受。这对于中国企业无论是在国内还是在境外发展都尤为重要。

本标准可指导未进行合规管理的组织确定、运行、评价和改进合规管理体系，也可对已建立合规管理体系的组织改进合规管理提供指导。本标准的合规管理体系流程图与其它管理体系一致，以持续改进原则为基础制定，见图 1。

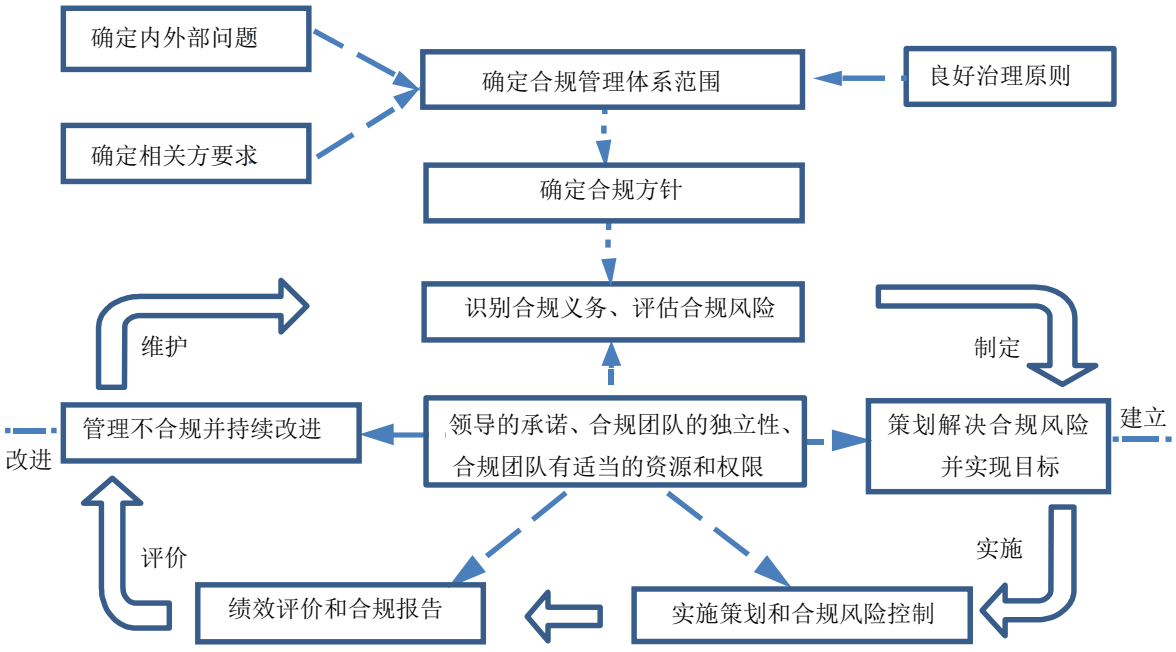

图1　合规管理体系流程图

本标准适用于所有类型的组织，它对组织合规管理不提出具体要求，只提供建立合规管理体系的指南和建议做法。

本标准除了为合规管理体系提供通用指南外，也为其他管理体系合规要求的具体实施提供框架，并帮助组织改进合规义务的整体管理。

未采用管理体系标准或合规管理框架的组织能轻松采用本标准作为组织的独立指南。

本标准能与现行管理体系标准（如：GB/T 19001、GB/T 24001 和 GB/T 22000）以及通用指南（如：GB/T 24353 和 GB/T 36000）结合使用。

合规管理体系　指南

1　范围

本标准旨在对组织内建立一套有效和及时响应的合规管理体系，并对其实施、评价、维护和改进提供指导。本标准适用于所有类型的组织。本标准的应用程度取决于组织的规模、结构、性质和复杂性。本标准以良好治理、比例原则 、透明性和可持续性原则为基础制定。

2　规范性引用文件

无规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

组织　organization

具有自身职能，并具有职责、权限和相互关系以实现其**目标**（3.9）的个人或团体。

注：组织的概念包括但不限于个体经营者，公司，集团，商行，企事业单位，权力机构，合伙企业， 慈善机构或研究机构，或上述组织的部分或组合，无论是否组成法人组织，无论公有还是私有。

3.2

相关方 interested party

利益相关方 stakeholder

能影响某个决定或活动的个人或**组织**（3.1）。

注：包括被影响或自己认为被影响的个人或组织（3.1）。

3.3

最高管理者 top management

在最高层指挥和控制**组织**（3.1）的个人或一组人。

注1：最高管理者在组织中拥有授权和提供资源的权力。

注2：如果**管理体系**（3.7）的范围只涉及组织的一部分，则其最高管理者是指挥和控制该组织这一部分的个人或一组人。

3.4

治理机构 governing body

对**组织**（3.1）进行治理、设定方向并对**最高管理者**（3.3）问责的个人或一组人。

3.5

员工 employee

国家法律或实践认可的雇佣关系中受雇的个人。

3.6

合规团队 compliance function

负责**合规**（3.17）管理的个人（或多个人）。

注：最好指定一个人全面负责**合规**（3.17）管理。

3.7

管理体系 management system

组织（3.1）的相互联系或相互作用的要素的组合，以确立组织的**方针**（3.8）、**目标**（3.9）和**过程**（3.10），并实现这些目标。

注1：一个管理体系能涉及一个方面或多个方面。

注2：本体系要素包括组织的结构、角色、职责、策划和运行等。

注3：管理体系的范围可包括整个组织、该组织具体和确定的职能、该组织具体和确定的部分或横跨一组组织的一个或多个职能。

3.8

方针 policy

由最高管理者正式表述的组织的总体意图和方向。

3.9

目标 objective

要实现的结果。

注1：目标分为战略、战术和/或操作目标。

注2：目标能与不同方面（如财务、健康和安全及环境的目标）相关，且能应用于不同层面（如战略层、整个组织、项目、产品和**过程**（3.10））。

注3：目标能用其它方式表达，如：预期成果、目的、操作依据，合规目标，或使用具有相似含义的其它词汇（如：目的、目标或指标）。

注4：在合规管理体系中，合规目标由组织确定，与合规方针一致，以实现具体结果。

3.10

过程 process

将输入转化为输出的相互关联或相互作用的一组活动。

3.11

风险 risk

不确定性对**目标**（3.9）的影响。

注1：影响是指偏离预期，可以是正面的或负面的。

注2：不确定性指对某事件及其后果或可能性的信息缺失或了解片面的状态。

注3：风险通常以潜在“事件 ”（GB/T 23694—2013 的 4.5.1.3）和“后果”（GB/T 23694—2013 的 4.6.1.3）或二者组合的特征来分析。

注4：通常用“事件”、“后果”（包括情形的变化）和事件发生的“可能性 ”（GB/T 23694—2013 的 4.6.1.1 的定义）的组合来表示风险。

3.12

合规风险 compliance risk

不确定性对于合规**目标**（3.9）的影响。

注：合规风险以组织**合规义务**（3.16）内的**不合规**（3.18）发生的可能性和后果表述。

3.13

要求 requirement

明示的、隐含的或必须履行的需求或期望。

注1：“隐含”是指**组织**（3.1）和**相关方**（3.2）的惯例或一般做法，这些需求或期望是不言而喻的。

注2：规定要求是指经明示的要求，如以文件化信息的形式。

3.14

合规要求 compliance requirement

组织（3.1）必须遵守的**要求**（3.13）。

3.15

合规承诺 compliance commitment

组织（3.1）选择遵守的**要求**（3.13）。

3.16

合规义务 compliance obligation

合规要求（3.14）或**合规承诺**（3.15）。

3.17

合规 compliance

履行组织的全部**合规义务**（3.16）。

注：通过将合规融入**组织**（3.1）文化及其工作人员的行为和态度中，使合规具有可持续性。

3.18

不合规 noncompliance

不履行某项**合规义务**（3.16）。

注：不合规能为单一事件或多项事件，且可为或可不为**不合格**（3.33）的结果。

3.19

合规文化 compliance culture

贯穿整个**组织**（3.1）的价值观、道德准则和信念，与组织的结构和控制系统相互作用，产生有利于**合规**（3.17）成果的行为准则。

3.20

准则 code

组织内部制定或由国际、国家、行业机构或其他**组织**（3.1）制定的表述惯例的文件。

注：准则可以是强制性或自愿性。

3.21

组织和行业标准 organizational and industry standards

组织认为相关的成文的**准则**（3.20）、良好惯例、章程、技术和行业标准。

3.22

监管机构 regulatory authority

负责管制或强制执行符合立法要求和其他要求的组织。

3.23

能力 competence

应用知识和技能取得预期结果的本领。

3.24

文件化信息 documented information

组织（3.1）要求控制和维护的信息和纳入媒介的信息。

注1：文件化信息指任何版式 、和媒介，且来源不限。

注2：文件化信息指：

——包括相关**过程**（3.10）的**管理体系**（3.7）；

——组织运行产生的信息（文件）；

——已实现结果的证据（记录）。

3.25

程序 procedure

为进行某项活动或**过程**（3.10）所规定的途径。

3.26

绩效 performance

可测量的结果。

注1：绩效可能是定量或定性的结果。

注2：绩效可能与活动的管理、**过程**（3.10）、产品（包括服务）、体系或**组织**（3.1）有关。

3.27

持续改进 continual improvement

改善**绩效**（3.26）的循环活动或**过程**（3.10）。

3.28

外包（动词）outsource (verb)

安排外部**组织**（3.1）执行组织部分职能或**过程**（3.10）。

注：尽管外包的职能或过程在管理体系之中，但外部组织在**管理体系**（3.7）之外。

3.29

监视 monitoring

确定系统、**过程**（3.10）或活动的状态。

注1：为确定状态可能需要进行检查、监督或密切观察。

注2：监视并非一次性活动，而是对某种情况定期或连续地观察的过程。

3.30

测量 measurement

确定量值的**过程**（3.10）。

3.31

审核 audit

为获取“审核证据”并对其进行客观的评价，以确定满足审核准则的程度所进行的系统的、独立的并形成文件的**过程**（3.10）。

注1：审核可分为内部审核（第一方）或外部审核（第二方或第三方），还可为联合审核（合并两个或多个方面）。

注2：“审核证据”和“审核准则”的定义见GB/T 19011。

注3：独立性指与正在被审核的活动无责任关系、对其无偏见和利益冲突。

3.32

合格（符合） conformity

满足管理体系**要求**（3.13）。

3.33

不合格（不符合）nonconformity

不满足管理体系**要求**（3.13）。

注：不合格不一定是**不合规**（3.18）。

3.34

纠正 correction

为处理已发现的**不合格**（3.33）或**不合规**（3.18）所采取的措施。

3.35

纠正措施 corrective action

为消除导致**不合格**（3.33）或**不合规**（3.18）发生的原因并防止其再发生所采取的措施。

4 组织背景

4.1 理解组织及其背景

组织宜确定其内部和外部问题，如与合规风险相关、与组织目标相关和影响组织实现合规管理体系预期成果能力的问题。这种情况下，组织宜考虑更大范围的内部和外部因素，如监管、社会和文化环境、经济形势、内部方针、程序、过程和资源。

4.2 理解相关方的需求和期望

组织宜确定：

——合规管理体系的相关方；

——这些相关方的要求。

4.3 确定合规管理体系的范围

组织宜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阐明应用合规管理体系的地域和/或组织边界，尤其该组织是某大规模组织在给定地点的分支机构时。

确定该范围时，组织宜考虑：

——4.1 提及的内部和外部问题；

——4.2 和 4.5.1 提及的要求。

范围宜是随时可用的文件化信息。

4.4 合规管理体系和良好治理原则

组织宜确立、制定、实施、评价、维护和持续改进合规管理体系，根据本标准并考虑如下治理原则，包括必需的过程和过程的相互作用：

——合规团队与治理机构建立直接联系；

——合规团队的独立性；

——分配给合规团队适当的权限和充足的资源。

合规管理体系宜反映组织的价值观、目标、战略和合规风险。

4.5 合规义务

4.5.1 合规义务的识别

组织宜系统识别其合规义务及其对组织活动、产品和服务的影响。组织在确立、制定、实施、评价、维护和改进合规管理体系时，宜考虑这些合规义务。

组织宜以适合其规模、复杂性、结构和运行的方式记录其合规义务。

合规义务的来源宜包括合规要求和合规承诺。

示例1：合规要求的示例包括：

——法律法规；

——许可、执照或其它形式的授权；

——监管机构发布的命令、条例或指南；

——法院或行政法庭的判决书；

——条约、惯例和协议。

示例2：合规承诺示例包括：

——与社区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；

——组织要求，如方针和程序；

——自愿原则或准则；

——自愿性标志或环境承诺；

——组织签署协议产生的义务；

——相关组织和行业标准。

4.5.2 合规义务的维护

组织宜有适当的过程识别法律、法规、准则和其它合规义务的出台和改变，确保持续合规。组织宜有序评价已识别的变更和任何变更的实施对合规义务管理的影响。

示例：获取法律和其它合规义务改变信息的过程包括：

——列入相关监管部门收件人名单中；

——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；

——关注监管部门网站；

——与监管部门会晤；

——与法律顾问洽商；

——关注合规义务来源（如：监管声明和法院判决）。

4.6 合规风险的识别、分析和评价

组织宜识别并评价其合规风险。该评价是正式合规风险评估或其他替换方法的基础。合规风险评估构成了合规管理体系实施的基础，是有计划地分配适当和充足的资源和管理已识别合规风险的基础。

组织识别合规风险，宜把合规义务和它的活动、产品、服务和运行的相关方面联系起来，以识别可能发生的不合规。组织宜识别不合规的原因及后果。

组织宜通过考虑不合规的原因、来源、后果的严重程度、不合规的可能性和可能产生的后果进行合规风险分析。后果包括，例如：个人和环境伤害、经济损失、声誉损失和行政责任。

风险评价涉及组织合规风险分析过程中发现的合规风险等级与组织可能并愿意接受的合规风险水平的比较。

基于这个比较，作为确定需要实施的控制（参见6.1）及其程度的优先级设定的基础。

发生以下情形，宜对合规风险进行周期性再评估：

合规风险评估宜周期性地重复进行或者在出现以下情形时随时进行：

——新的或改变的活动、产品或服务；

——组织结构和战略改变；

——重大的外部变化，例如金融经济环境、市场条件、债务和客户关系；

——合规义务改变（参见 4.5）；

——不合规。

注1：合规风险评估细节的程度和水平取决于组织的风险情况、环境、规模和目标，并可在特定方面（如环境、财务和社会）进行变化。

注2：基于风险的合规管理方法不意味着在低合规风险情况下不合规可被组织接受。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，最终涵盖所有合规风险。所有已识别的合规风险/情况需监视、纠正和纠正措施。

注3：GB/T 24353 给出了风险评估详细指南。

5 领导

5.1 领导和承诺

治理机构和最高管理者宜通过下列方式证明其对合规管理体系的领导和承诺：

a) 确立和坚持组织的核心价值观；
b) 确保确立组织的合规方针和合规目标，并与该组织（参见 6.2）的价值观、目标和战略方向保持一致；
c) 确保制定并实施合规方针、程序和过程，以实现合规目标；
d) 确保合规管理体系所需资源的可用、分配和指派；
e) 确保合规管理体系要求融入组织的业务流程；
f) 传达有效合规管理体系的重要性和符合合规管理体系要求的重要性；
g) 指导和支持人员提升合规管理体系的有效性；
h) 支持其他相关管理者，使他们在自己担责的领域中展现出合规领导力；
i) 确保运行指标和合规义务保持一致；
j) 确立并维护问责机制，包括对合规事件和不合规及时报告；
k) 确保合规管理体系实现它的预期成果；
l) 推进持续改进。

示例：有效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。承诺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行动和决定，积极证明他们承诺确立、制定、实施、评价、维护和改进的是一个有效和及时响应的合规管理体系；

——合规方针经治理机构正式批准；

——最高管理者承担责任，确保组织合规的承诺充分实现；

——所有管理层一致向员工传达一个清晰的信息（通过文字和行动）：组织将履行它的合规义务；

——以清晰并令人信服的声明广泛传达合规承诺，并有行动支持；

——合规团队被赋予一定级别的权限，这反映有效合规的重要性且合规团队可直接向治理机构报告；

——通过增强活动意识和培训，分配资源确立、制定、实施、评价、维护和改进强健的合规文化；

——方针、程序和过程不仅反应法律要求，还包括自律守则和组织的核心价值观；

——组织向其所有管理层分配合规责任并要求他们负责；

——要求对合规管理体系进行定期评审；

——组织的合规绩效被持续改进；

——采取纠正措施。

5.2 合规方针

5.2.1 概述

治理机构和最高管理者（更适宜与员工协商）宜确定合规方针：
——适合于组织目的；
——为设定合规目标提供框架；
——包括满足适用要求的承诺；
——包括持续改进合规管理体系的承诺。
合规方针宜明确：
——合规管理体系的范围；
——与组织规模、性质、复杂性和运行环境有关的体系运用与体系环境；
——合规与其他职能，如治理、风险、审核和法律的结合程度；
——合规融入运行的方针、程序、过程的程度；
——合规团队的独立和自治程度；
——管理和报告合规事项的责任；
——管理内部和外部利益相关方关系的原则；
——所要求的行为和问责的标准；
——不合规的后果。
合规方针宜：
——作为文件化信息可供使用；
——以通俗易懂的语言书写，便于所有员工均能容易地理解原则和目的；
——如必要翻译为其它语言；
——在组织内明确传达，且所有员工可随手获得；
——由相关方获得，如适当；
——按要求更新，以确保保持相关性。
确立的合规方针宜与组织的价值观、目标和战略保持一致，且宜通过治理机构批准。
合规方针确立组织实现合规的总原则和行动承诺。它设定要求的责任和绩效水平以及评估行动的期望。方针宜适合于组织活动产生的合规义务。
合规方针不宜是孤立的文件，宜由其它文件支持，包括运行方针、程序和过程。

5.2.2 制定

制定合规方针，宜考虑：
a) 国际、区域或本地的特定义务；
b) 组织的战略、目标和价值观；
c) 组织的结构和治理框架；
d) 与不合规有关的风险性质和等级；
e) 其它内部方针、标准和准则。

5.3 组织的角色、职责和权限

5.3.1 概述

最高管理者宜确保相关角色的职责和权限在组织内分配和明晰。
治理机构和最高管理者宜为合规团队分配职责和权限，以：
a) 确保合规管理体系与本标准一致；
b) 向治理机构和最高管理者报告合规管理体系的绩效。

注：合规团队的特定责任并不减轻其他员工对可能存在的合规报告的职责。

5.3.2 组织内分配的合规职责

治理机构和最高管理者的积极参与和监督是有效合规管理体系不可分割的一部分。这有助于确保员工充分理解组织的方针和运行程序，以及如何将其运用在他们的工作中，并确保他们有效地履行合规义务。

要使合规管理体系有效运行，治理机构和最高管理者需要通过坚持积极地支持合规和合规管理体系来以身作则。

许多组织由专人（如：合规专员）负责日常的合规管理，有些组织由跨职能的合规委员会协调整个组织的合规工作。

一些组织（取决于其规模）有人员全面负责合规管理，尽管这可能是其他角色或职能之外的职责，包括现有委员会、组织部门、也有的组织把部分工作外包给合规专家。

这不宜被视为免除了其他管理层的合规职责，因为所有管理者对合规管理体系都发挥一定的作用。因此，在他们的职位描述中清晰地设定他们各自的职责十分重要。

管理者的合规职责必然地会随着权限、影响力和其它因素的水平而变化，如组织的性质和规模。但是，有些职责有可能是各类组织共有的。

注： 本标准并未区分职责和问责的概念。使用“职责”这一术语暗示了问责的含义。

5.3.3 治理机构和最高管理者的角色和职责

治理机构和最高管理者宜：

a) 根据 5.2.2 条确立合规方针；
b) 确保维护合规承诺，并确保恰当处理不合规和不合规行为；
c) 将合规职责纳入最高管理者职位描述；
d) 任命或提名一个合规团队：
    1) 具有合规管理体系的设计、一致性和完整性的权限和职责；
    2) 有权直接访问治理机构和最高管理者和获得来自他们的清晰和明确的支持；
    3) 使其有权限接触：
    - 高级决策制定者并在决策制定初期提供意见和建议；
    - 组织的各个层面；
    - 执行合规任务所需的所有文件化信息和数据；
    - 相关法律、法规、准则和组织标准的专家建议；
    - 确保建立高效及时的报告系统。
    4) 通过展示相关决策过程所造成的任何合规后果，实施抗衡力量的权限和能力；
e) 确保合规团队具备独立采取行动的权限，且该职能不会受到优先级冲突的影响，特别是当合规已融入该组织业务的情况下。

最高管理者宜：

——分配充足和适当的资源以确立、制定、实施、评价、维护和改进合规管理体系及绩效成果；
——确保组织分配和传达相关角色的职责和权限
——对照合规关键绩效考核或成果测量
——分配向治理机构和最高管理者报告合规管理体系绩效的合规职责。

5.3.4 合规团队

不是所有的组织都会创建独立的合规团队，某些组织可将此职能分配给现有职位。

合规团队宜与管理者合作，负责以下事宜：

a) 在相关资源的支持下识别合规义务，并将那些合规义务转化为可执行的方针、程序和过程；
b) 将合规义务融入现有的方针、程序和过程；
c) 为员工提供或组织持续培训，以确保所有相关员工得到定期培训；
d) 促进合规职责融入职位描述和员工绩效管理过程；
e) 设定适当的合规报告和文件化体系；
f) 制定和实施信息管理过程，如通过热线、举报系统和其它机制进行投诉和/或反馈；
g) 确立合规绩效指标，监视和测量合规绩效；
h) 分析绩效以识别需要采取的纠正措施；
i) 识别合规风险，并管理与第三方有关的合规风险，如供应商、代理、分销商、咨询顾问和承包商；
j) 确保按计划定期对合规管理体系进行评审；
k) 确保合规管理体系的建立、实施和维护能得到适当的专业建议；
l) 使员工可以得到与合规程序和参考资料相关的资源；
m) 对合规相关事宜向组织提供客观建议。

注：GB/T 19012提供投诉处理指南。

分配合规管理职责，宜考虑确保与合规团队无利益冲突，并已证明：

——诚信和信守合规；
——有效沟通和影响技能；
——能力和身份，使建议和指南的命令被接受；
——相关能力。

5.3.5 管理职责

管理层宜负责其职责范围内的合规。这包括：

a) 与合规团队合作并支持合规团队，鼓励员工也这样做；
b) 个人遵守并被看到遵守方针、程序、过程、参加和支持合规培训活动；
c) 在运营中识别和交流合规风险；
d) 积极承担并鼓励监视、辅导和监督员工以促进合规行为；
e) 鼓励员工提出其所关注的合规问题；
f) 积极参与合规相关事件和问题的管理和解决；
g) 提高员工合规义务的意识，并指导员工满足培训和能力要求；
h) 确保合规写入职位描述；
i) 将合规绩效纳入员工绩效考核（如：关键绩效指标、指标和晋升准则）；
j) 将合规义务纳入他们职责范围内的现有业务实践和程序；
k) 与合规团队协力，确保一旦认定需要纠正措施，则实施；
l) 对外包业务进行监督，确保合规义务被纳入考量。

5.3.6 员工职责

包括管理者在内的所有员工宜：

a) 坚持履行与其职位和职务有关的组织合规义务；
b) 按照合规管理体系要求参与培训；
c) 使用可获得的作为合规管理体系一部分的的合规资源；
d) 报告合规疑虑、问题和失败。

6 策划

6.1 合规风险的应对措施

组织进行合规管理体系策划，宜考虑4.1提及的问题，4.2提及的要求，4.4提及的良好治理原则，4.5识别的合规义务，4.6提及的合规风险评估结果，以确定需解决的合规风险，以：

——确保合规管理体系能实现预期成果；

——防范、监察并减少不希望的效果；

——实现持续改进。

组织宜计划：

——应对合规风险的措施；

——如何：

a) 将行动纳入合规管理体系过程并实施；

a) 评价这些行动的有效性。

组织宜保留与合规风险和解决合规风险的计划的行动相关的文件化信息。

6.2 合规目标和实施策划

组织宜确立相关职能部门和层面的合规管理体系目标。

合规目标宜：

a) 与合规方针一致；

b) 可测量（如可行）；

c) 考虑适用的要求；

d) 在监视下；

e) 充分沟通；

f) 适当时，更新和/或修订。

组织策划如何实现合规目标时，宜确定：

——做什么；

——需要什么资源；

——谁负责；

——何时完成；

——结果如何评价，如：根据已识别的合规关键绩效考核或成果测量。

组织宜保留关于合规目标和实现合规目标的计划行动的文件化信息。

7 支持

7.1 资源

组织宜确定并提供确立、制定、实施、评价、维护和持续改进合规管理体系的资源，合规管理体系宜适合于组织的规模、复杂性、结构和运营。

最高管理者和各管理层宜确保有效部署必要的资源，以确保满足合规管理体系目标，并实现合规。

资源包括财务的和人力的资源，外部建议和专业技能，组织基础设施，关于合规管理和法律义务、专业发展和技术的现时参考资料。

7.2 能力和培训

7.2.1 能力

组织宜：

1) 确定员工必备的影响合规管理体系绩效的工作能力；
2) 确保这些员工在适当的教育、培训和/或工作经验的基础上能胜任工作；
3) 在适用的情况下，采取行动获得必要的能力，并评价所采取行动的有效性；
4) 保存适当的文件化信息，包括能力证明。

注：适用的行动能包括，例如：对员工的培训、指导或调岗；或雇佣与聘用合格人员。

7.2.2 培训

有合规义务的治理机构、管理层和所有员工都宜具备有效履行合规义务的能力。能通过多种方式获得能力，包括通过教育、培训或工作经历获取必需的技能和知识。

培训项目的目标是确保所有员工有能力以与组织合规文化和合规承诺一致的方式履行岗位职责。

设计合理并有效执行的培训能为员工提供有效的方式了解之前未识别的合规风险。

对员工的教育和培训宜：

a) 针对员工角色和职责相关的义务和合规风险；
b) 在适当时，以对员工知识和能力缺口的评估为基础；
c) 在组织成立时就提供并持续提供；
d) 与组织的培训计划一致，并纳入年度培训计划；
e) 实用并易于员工理解；
f) 与员工的日常工作相关，并且以相关行业、组织或部门的情况作为案例；
g) 足够灵活，涉及各种技能，以满足组织和员工的不同需求；

注：如果不合规能导致严重的后果，互动培训可能是最好的培训方式。

h) 评估有效性；
i) 按要求更新；
j) 记录并保存。

宜考虑合规再培训，每当：

——岗位或职责改变；
——内部方针、程序和过程改变；
——组织结构改变；
——合规义务尤其是法律或相关方要求改变；
——活动、产品或服务改变；
——发生监视、审核、评审、投诉和不合规，包括利益相关方反馈。

7.3 意识

7.3.1 概述

在组织控制下工作的人员宜清楚：

a) 合规方针；
b) 他们的角色和对合规管理体系有效性的贡献，包括改善合规管理体系绩效的效益；
c) 不符合合规管理体系要求的后果。

7.3.2 行为

7.3.2.1 概述

宜鼓励创建和支持合规的行为，不宜容忍危害合规的行为。

7.3.2.2 最高管理者在鼓励合规中的角色

最高管理者的关键职责：

a) 调整组织的合规承诺，与组织的价值观、目标和战略一致，以便恰当地定位合规合；
b) 宣传组织的合规承诺，以便建立员工接受合规管理体系的自觉性和热情；
c) 鼓励所有员工接受，实现他们所负责或应负责的合规目标的重要性；
d) 创造一个鼓励报告不合规并且报告的员工不会受到报复的环境；
e) 鼓励员工提有利于合规绩效持续改进的建议；
f) 确保合规已融入更广泛的组织文化以及文化改变的计划中；
g) 迅速识别并采取行动纠正和解决不合规；
h) 确保组织方针、程序和过程支持和鼓励合规；
i) 确保运营目标和指标不会危害合规行为。

7.3.2.3 合规文化

发展合规文化要求治理机构、最高管理者和管理层，对组织的各个领域所要求的共同的、已发布的行为标准作出积极的、可见的、一致的和持久的承诺。

示例：支持合规文化发展的因素的例子包括：

——一系列已发布的清晰的价值观；
——管理层积极实施和遵守价值观；
——不论职位，处理相似行动时保持一致；
——在监视、指导和领导过程中以身作则；
——对潜在员工进行适当的就业前评估；
——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，包括更新培训内容；
——持续就合规问题进行沟通；
——建立绩效考核体系，考虑对合规行为的评估，并将合规表现与工资挂钩，以实现合规关键绩效指标和结果；
——对合规管理业绩和成果予以明显认可；
——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惩罚；
——在组织战略和个人角色之间建立清晰的联系，反映出合规是实现组织成果所必不可少的；
——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：

——所有上述事项均得到充分实施；
——利益相关方（尤其是员工）相信上述事项已得到充分实施；
——员工充分了解其自身行为相关的合规义务以及所在其业务部门相应的合规义务；
——组织各层按要求针对不合规进行“自主”补救，并采取相应措施；
——合规团队所扮演的角色及其目标得到重视；
——员工有能力且受到鼓励向相应的管理层提出其合规疑虑。

7.4 沟通

7.4.1 概述

组织宜确定与合规管理体系相关的内部和外部的沟通需求，包括：

a) 沟通内容；
b) 沟通时间；
c) 沟通对象；
d) 沟通方式。

注：关于内部和外部合规报告的指南参见9.1.7和9.1.8。

7.4.2 内部沟通

组织宜采用适当的沟通方式，以确保全体员工持续获知并理解合规信息。沟通宜明确给出组织对员工的期望，预计不合规将在何种情形下逐级上报给谁。

7.4.3 外部沟通

宜根据组织方针采用实用的方法与所有相关方进行外部沟通。

相关方能包括但不限于：监察机构、客户、承包商、供应商、投资方、紧急服务提供方、非政府组织和邻居。

沟通方式可包括通过网站和电子邮件、新闻稿、广告和定期简报、年度（或其它定期）报告、非正式讨论、开放日、分组座谈会、社区对话、参与社区活动，和热线电话。这些方式能鼓励（相关方）理解和接受组织的合规承诺。

7.5 文件化信息

7.5.1 概述 general

组织的合规管理体系宜包括：

a) 本标准推荐的文件化信息；
b) 组织确定合规管理体系有效所必须的文件化信息。

示例：文件化信息包括：

——组织的合规方针；

——合规管理体系的目标、指标、结构和内容；

——合规职责和角色分配；

——相关合规义务登记；

——根据合规风险评估过程进行合规风险登记并确定优先处理顺序；

——登记不合规和近乎违规行为；

——年度合规计划；

——人事记录，包括但不限于培训记录。

注1：文件化信息能包括监管报告要求相关事项。

注2：不同组织合规管理体系文件化信息的程度不同，可能因为：

——组织规模和它的活动、过程、产品和服务的类型；

——过程和过程间相互作用的复杂性；

——员工的能力；

——合规管理体系的成熟度。

7.5.2 新建和更新

新建和更新文件化信息时，组织宜确保适当的：

——标示和描述（例如：标题、日期、作者、参考资料或版本号）；

——格式（例如：语言、软件版本和图形）和媒介（例如：纸张或电子）；

——适用性和充分性的评审和批准。

7.5.3 文件化信息的控制

宜对合规管理体系和本标准推荐的文件化信息进行控制，以确保：

a) 何时何处需要时，它便于、易于和适于取用；

b) 它得到充分地保护（例如：避免泄露机密、不当使用或失去完整性）。

对于文件化信息的控制，如适用，组织宜进行以下活动：

——分发、获取、检索和使用；

——文件保存，包括字迹的保持；

——对变更的控制（例如：版本控制）；

——保留、处置和处理；

——文件化信息的新建和控制中第三方的角色。

组织确定的对于计划和运行合规管理体系所必须的外部来源的文件化信息，宜适当的被识别和控制

可本着获取法律建议或取得法律特权的目的来对文件化信息进行编制。

注：使用权指关于只允许查看文件化信息的决定或允许并授权查看和更改文件化信息等的决定。

8 运行

8.1 运行的策划和控制

组织宜计划、实施和控制满足合规义务必需的过程， 并实施6.1条确定的行动，通过：

——确定过程的目标；

——确立过程的依据；

——根据准则实施过程控制；

——记录必要的文件化信息，确信过程已按计划实施。

组织宜控制计划变更，并重新评审计划外变更的后果，必要时采取措施缓解任何不利影响

8.2 建立控制和程序

落实控制措施，管理确认的合规义务和对应的合规风险，实现预期的行为

采取有效的控制措施确保满足组织的合规义务，能够预防或发现不合规事件并纠正。充分而严格的设计各类、各层次的控制措施，以促进组织的活动和经营环境实现具体的合规义务。在合理的情况下，这些控制宜植入正式的组织流程。

示例：控制的示例包括：

——清晰、实用并易于遵循的文件化运行方针、程序、流程和说明；

——体系和异常报告；

——审批；

——划分有冲突的岗位和职责；

——自动化过程；

——年度合规计划；

——员工绩效计划；

——合规评估和审核；

——管理层对的以身作则和表率和促进合规行为的其他措施；

——对预期的员工行为（标准、价值观和行为准则）进行主动、公开并经常的沟通。

宜维护、定期评价并试验这些控制，以确保控制的持续有效。

宜确立程序，文件化，执行并维护，以支持合规方针，实践合规义务。

制定这些程序宜考虑：

a) 将合规义务整合到程序中，包括计算机系统、表格、报告系统、合同和其它法律文件；

b) 与组织的其它评审和控制职能保持一致；

c) 持续监视和测量；

d) 评估和报告（包括管理监督）以确保员工遵守程序；

e) 专门安排识别、报告和逐级上报不合规实例和不合规风险。

8.3 外包过程

组织宜确保外包过程受到控制和监视。

组织的运行外包通常不减轻组织的法律职责或合规义务。如果组织将任何活动外包，组织需要执行有效的尽职调查，以确保不会降低组织标准和合规承诺。宜对承包商进行适当控制，以确保有效遵守合同（例如，第三方绩效考核）。

组织宜考虑与过程有关的第三方相关的合规风险，如产品和服务供应，产品分销，和在必要的情况下的适当控制（例如，合同条款的合规义务）。

9 绩效评价

9.1 监视、测量、分析和评价

9.1.1 概述

组织宜确定：

a) 需要被监视和测量的内容和原因；

b) 监视、测量、分析、评价的方法（如适用），以确保有效的结果；

c) 何时宜进行监视和测量；

d) 何时宜分析、评价和报告监视和测量的结果。

组织宜适当保留文件化信息，作为结果证据。

组织宜评价合规管理体系的绩效和合规管理体系的有效性。

9.1.2 监视

宜监视合规管理体系以确保实现合规绩效。宜制定持续监视计划，设定监视过程、时间表、资源和要收集的信息。

合规监视是为了评估合规管理体系有效性和组织合规绩效，收集信息的过程。

典型的合规管理体系监视包括：

——培训的有效性；

——控制的有效性，如：抽样检查的结果；

——有效分配满足合规义务的职责；

——合规义务的宣贯程度；

——确认原先处理合规失败的有效性；

——内部合规检验未按时间表执行的案例。

典型的合规绩效监视包括：

——不合规和“近乎违规行为”（即未造成负面影响的事件）；

——未履行合规义务的案例；
——未实现目标的案例；
——合规文化的情况；
——9.1.6 条确立的领先和滞后指标。

9.1.3 合规绩效反馈来源

组织宜建立、实施、评价和维护用以寻求和接收合规绩效反馈信息的程序，反馈来源包括：
——员工，例如，通过举报设施、热线电话、反馈和意见箱；
——客户，如通过投诉处理系统；
——供应商；
——监管部门；
——过程控制日志和活动记录（包括电脑和纸质）。

示例：合规绩效反馈的例子包括：
——合规问题；
——不合规和合规疑虑；
——新出现的合规问题；
——持续监管和组织的变更；
——对合规有效性和合规绩效的评论。

反馈宜是持续改进合规管理体系的重要来源。

9.1.4 信息收集方法

许多方式可收集信息。不同情况下，下列每种方法是相关的，宜谨慎选择适用于组织大小、规模、性质和复杂性的工具。

示例：信息收集的例子包括：
——出现或确认不合规时的特别报告；
——通过热线电话、投诉和其它反馈（包括举报）所收集的信息；
——漫谈会、研讨会和分组座谈会；
——抽样和诚信试验，例如神秘购物；
——感觉调查的结果；
——直接观察、正式访谈、工厂巡视和检查；
——审核和评审；
——利益相关方质询、培训要求和培训过程中的反馈（尤其是员工的反馈）。

9.1.5 信息分析和分类

对信息的有效分类和管理至关重要。
宜建立信息的分类、存储和检索系统。

示例：信息分类准则的例子包括：
——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。

信息管理体系宜同时收集问题和投诉，并允许对合规相关的信息进行分类和分析。

一旦收集了信息，需要对它进行分析和精确评估以确定根本原因和需采取的适当行动。分析宜考虑系统性和反复发生的问题，并进行改正或改进，因为这些可能给组织带来重大并更加难以识别的合规风险。

9.1.6 指标制定

组织确定一系列可衡量指标具有十分重要的意义，此类指标可帮助组织对其目标的实现程度（参见6.2）进行衡量，并量化合规绩效。该过程宜参考合规风险的评估结果（参见4.6），以确保各指标与该组织的合规风险特征具有相关性。合规绩效测量内容和方式的问题，从某些方面而言具有挑战性，然而，这是证明合规管理体系有效性的重要部分。而且，必要的指标将随组织的成熟度、时机和新的、改进的程序实施程度而改变。

示例1：活动性指标的例子包括：

——经过有效培训的员工比例；

——监管部门联系的频率；

——反馈机制的使用（包括用户对那些机制价值的评论）；

——对于每项不合规，采取何种类型的纠正措施。

示例2：反应性指标的例子包括：

——根据类型、区域和频率报告已识别的问题和不合规；

——不合规的后果，包括对货币补偿、罚款和其它处罚、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。

示例3：预测性指标的例子包括：

———定时期的不合规风险（测量目标（收益、健康和安全、声誉等）的潜在损失/收获）；

——不合规趋势（基于过去趋势预测合规率）。

9.1.7 合规报告制度

a) 治理机构、管理层和合规团队宜确保他们能够及时有效并持续充分地了解组织合规管理体系绩效，包括所有相关的不合规，并及时和积极地推动这一原则：组织鼓励和支持充分和坦诚报告的文化。内部报告制度的安排宜确保：设定适当的报告准则和义务；
b) 确立定期报告时间表；
c) 建立便于对新出现的不合规进行特别报告的异常报告系统；
d) 合适的系统和过程确保信息的准确性和完整性；
e) 向组织的适当职能部门或区域提供准确和完整的信息，以采取预防、纠正和补救措施。
f) 要对向治理机构提交报告的准确性签字确认，包括合规团队的签字。

除非法律另有规定，组织宜选择适合自己情况的内部合规报告的版式、内容和时间。

对合规的报告宜融入组织的常规报告中。

只宜为重大不合规或新出现的问题单独编写报告。

需要对所有不合规做适当报告。尽管系统性和反复出现的问题特别重要，如果一次性不合规非常重大或故意为之，同样需要重视。即使一个小失败，可表明当前过程和合规管理体系存在严重缺陷。如果不及时报告，可能导致人们认为失败不重要并导致这样的失败成为系统性问题。

宜鼓励员工反映并报告违法行为和其它不合规事件，并将报告视为积极的，不构成威胁的行动，而无须担心遭到报复。

宜在组织的合规方针和程序中清晰地设定报告义务，并通过其它方法加以强化，例如由管理者在日常工作中对员工的非正式强化。

9.1.8 合规报告的内容

合规报告包括：

a) 组织按要求向任何监管机构通报的任何事项；
b) 合规义务变化及其对组织的影响，以及为了履行新义务，拟采用的行动方案；
c) 对合规绩效的测量，包括不合规和持续改进；
d) 可能的不合规数量和详细内容和随后对他们的分析；
e) 采取的纠正措施；
f) 合规管理体系有效性、业绩和趋势的信息；
g) 与监管部门的接触和关系进展；
h) 审核结果和监视活动。

合规方针宜促进常规报告时间表范围之外的实质性重大事件的立即报告。

9.1.9 记录

宜准确、即时地记录组织合规活动，这有助于监视和评审过程，并证明与合规管理体系的一致性。

记录宜包括对投诉、争议、宣称的不合规和解决它们的步骤的记录，并对其进行分类。

宜以确保清晰、容易、可辨认和可检索的方式保存记录。

宜保护这些记录，使其免于被增加、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：

a) 合规绩效信息，包括合规报告；
b) 来自相关方的投诉、解决方案和沟通；
c) 不合规及纠正和预防措施的详细内容；
d) 对合规管理体系和采取行动的评审和审核的结果。

9.2 审核

组织宜至少在计划的时间间隔内安排审核，以提供信息，确定合规管理体系是否：

a) 符合：
    1) 组织自身的合规管理体系依据；
    2) 本标准的建议；
b) 有效实施和维护。

也能按要求进行额外审核。

组织宜：

——计划、确立、实施、维护和审核程序，包括频率、方法、职责、计划要求和报告。审核程序宜考虑相关过程的重要性和前期审核的结果。
——规定审核准则和每次审核的范围；
——选择审核员，并进行审核，以确保审核过程的客观和公正；
——确保审核结果报告给相关管理层；
——保留文件化信息，作为实施审核程序和审核结果的证据。

9.3 管理评审

最高管理者宜按计划定期评审组织的合规管理体系，以确保其持续的适用性、充分性和有效性。此类评审的实际深度和频率将随组织的性质和方针变化。

管理评审宜考虑：

a) 以前管理评审行动的状态；

b) 合规方针的充分性；

c) 合规目标实现的程度；

d) 资源的充分性；

e) 与合规管理体系相关的内外部问题的变化

f) 合规绩效信息包括以下各项的趋势：

——不合格、纠正措施和解决的时间表；

——监视和测量结果；

——与相关方的沟通，包括投诉；

——审核结果；

g) 持续改进的机会。

管理评审的输出宜包括与持续改进机会相关的决定和合规管理体系所需的任何改动。

还宜包括以下方面的建议：

a) 合规方针所需的改变，它与目标、体系、结构和人员相关；

b) 合规过程的改变以确保与运行实践和体系有效整合；

c) 宜监视的未来潜在不合规可发生的区域；

d) 与不合规相关的纠正措施；

e) 当前合规管理体系和长期持续改进的目标之间的差距和不足；

f) 认可组织内的示范性合规行为。

组织宜保留文件化信息作为管理评审结果的证据，并宜向治理机构提交副本。

10 改进

10.1 不合格、不合规和纠正措施

10.1.1 概述

发生不合格和/或不合规时组织宜：

a) 对不合格和/或不合规做出反应，在适用情况下：

——采取行动控制和纠正它；

——管理后果；

b) 评价是否需要采取行动，消除不合格和/或不合规的根本原因，为了避免再次发生或在其它地方发生，通过：

——评审不合格和/或不合规；

——确定不合格和/或不合规的原因；

——确定是否存在或有可能发生类似的不合格和/或不合规；

c) 实施任何必要的行动；

d) 评审所采取的任何纠正措施的有效性；

e) 如必要，修改合规管理体系。

未能避免或发现一次性不合规并不一定意味着合规管理体系预防和发现不合规总体无效。

纠正措施宜适合于发生的不合格和/或不合规造成的影响。组织宜保留文件化信息，作为以下方面的证据：

——不合格和/或不合规的性质和随后采取的任何行动；

——任何纠正措施的结果。

通过分析不合格和/或不合规所得的信息能用于考虑：

——评估产品和服务绩效；

——改进和/或重新设计产品和服务；

——改变组织惯例和程序；

——对员工进行再培训；

——对通知相关方的必要性进行再评估；

——对潜在不合规提供早期预警；

——对控制进行重新设计或评审；

——强化通知和上报步骤（内部和外部）。

10.1.2 上报

宜采用并宣传清晰、及时的上报过程，以确保所有不合规都能被提出、报告并最终上报给相关管理层，并确保合规团队得到通知并能够为上报提供支持。在适当的情况下，宜向最高管理者和治理机构上报，其中包括相关委员会。该过程宜详细说明报告的对象、方式和时间以及内部和外部报告的时间表。

当组织需按法律要求报告不合规时，需根据适用法规或其他商定方式，通知监管机构。

即使法律未要求组织报告不合规，组织也可考虑自愿向监管机构自我披露不合规，以减轻不合规的后果。

有效的合规管理体系宜包括一种机制，使组织的员工和/或其他人以保密的方式报告可疑或实际的不当行为或违反组织合规义务，而无须担心遭到报复。

10.2 持续改进

组织宜设法持续改进合规管理体系的适用性、充分性和有效性。

宜将合规报告中对已收集信息进行的分析和相应评价作为识别该组织合规绩效改进机会的依据。

参 考 文 献

[1] GB/T 19001质量管理体系 要求（ISO 9001，IDT）
[2] GB/T 19012质量管理 顾客满意度 组织处理投诉指南（ISO 10002，IDT）
[3] GB/T 24001环境管理体系 要求及使用指南（ISO 14001，IDT）
[4] GB/T 19011质量和或环境管理体系审核指南（ISO 19011，IDT）
[5] GB/T 22000 食品安全管理体系 食品链中各类组织的要求（ISO 22000，IDT）
[6] GB/T 36000 社会责任指南（ISO 26000，MOD）
[7] ISO 31000 Risk management — Principles and guidelines
[8] GB/T 23694——2013 风险管理术语（ISO Guide 73:2009，IDT）