ISO37301:2021

合规管理体系要求及使用指南

1 范围

本文档详细说明了要求，并提供了在组织内建立，开发，实施，评估，维护和改进有效合规管理系统的指南。

本文档适用于所有类型的组织，无论活动的类型，规模和性质如何，以及该组织来自公共部门，私营部门还是非营利部门。

如果组织没有独立的理事机构，则本文档中指定的涉及理事机构的所有要求均适用于高层管理人员。

2 规范性引用

本文档中没有规范性引用。

3 术语和定义

就本文档而言，以下术语和定义适用。

ISO和I EC在以下地址维护用于标准化的术语数据库：

— ISO在线浏览平台：可从https://www.iso.org/obp获得

— IEC Electropedia：可在http://www.electropvdia.org/获得

3.1
组织
具有职责，权限和关系以实现其目标的职能的个人或一群人

注释1：组织的概念包括但不限于独资，公司，公司，公司，企业，机构，合伙企业，慈善机构或机构，或其一部分或组合，无论是否成立，公共或私人的。

注释2：如果组织是较大实体的一部分，则术语“组织”仅指在合规管理系统范围内的较大实体的一部分。

3.2
利害关系方（优先条款）
利益相关者**（允许的期限）**
可能会影响，感知到或被决策或活动影响的个人或组织

3.3
高层管理人员
在最高级别指导和控制*组织*的*个人*或一群人

注释1：最高管理者有权在组织内委派权限并提供资源。

注释2：如果*管理系统*（站）
的范围仅覆盖组织的一部分，则高层管理人员是指指导和控制组织的该部分的人员。

注释3：就本文档而言，术语“最高管理人员**”是指最高级别的执行管理人员。

3.4
管理系统
*组织*的一组相互关联或相互作用的元素，用于建立*策略*和*目标*以及实现这些目标的*过程*

注释1：管理系统可以处理一个或多个学科。

注释2：管理系统元素包括组织的结构，角色和职责，计划和运营。

3.5

政策
*组织*最高管理者正式表达的*组织*的*意图和方向*

注释1：策略也可以由组织的*理事机构*正式表达。

3.6
客观的
要达到的结果

注释1：目标可以是战略性，战术性或操作性的。

注释2：目标可以涉及不同的学科（例如金融，健康和安全以及环境）。例如，它们可以在整个组织范围内，或特定于项目，产品，服务或*过程*（服））·

注释3：目标可以用其他方式表示，例如作为预期结果，目的，操作准则，作为*达标情况*的目标，或通过使用具有相似含义的其他词语（例如目标，目的或目标）。

注释4：在合规*管理系统*中，组织应设定合规目标与合规*政策*一致，以取得特定结果。

3.7
风险
不确定性对目标的影响

注释1：影响是与预期的偏差-正或负。

注释2：不确定性是指与事件，其后果或可能性有关的信息，了解或知识的缺乏状态，甚至是部分的。

注释3：风险的特征通常是参考潜在的“事件”（如ISO指南73中定义）和“后果”（如ISO指南73中定义），或综合考虑。

注释4：风险通常表示为事件后果（包括环境变化）和相关的“可能性”（如ISO指南73中定义）的组合。

3.8
过程
一组相互关联或交互的活动，这些活动使用或转换输入以提供结果

注释1：过程的结果称为输出，产品还是服务取决于引用的上下文。

3.9
权限
应用知识和技能以达到预期结果的能力

3.10
书面信息
组织要求控制和维护的*信息*以及包含该信息的媒体

注释1：记录的信息可以采用任何格式和媒体，并且可以来自任何来源。

注释2：记录的信息可以参考：

— *管理系统*，包括相关*过程*；

— 为组织运作而创建的信息（文档）；

— 取得成果的证据（记录）。

3.11
表现
可测量的结果

注释1：绩效可能与定量或定性发现有关。

注释2：绩效可能与管理活动，*流程*，产品，服务，系统或*组织*有关。

3.12
持续改进
经常性活动以提高*绩效*

3.13
效力
实现计划的活动和达到计划的结果的程度

3.14
要求
所陈述的需求或期望，通常是隐含的或强制性的

注释1：“一般隐含的[1] *表示隐含在考虑中的需求或期望对于*组织*和*相关方*是一种惯例或惯例。

注2：规定的要求是已陈述的要求，例如在*书面信息*中。

3.15
符合
满足*要求*；

3.16
不合格
未满足*要求*

注1：不合格不一定是*不合格*。

3.17
纠正措施
消除不合格的原因并防止再次发生的措施

3.18
审计
系统和独立的*过程*，用于获取证据并对其进行客观评估，以确定满足审核标准的程度

注释1：审核可以是内部审核（第一方）或外部审核（第二方或*第三方*）。并且可以是合并审核（合并两个或多个学科）。

注释2：内部审核由*组织*（3JJ本身；或由外部团体代表组织）进行。

注释3：“审核证据[1] *和”审核标准”在ISO 19011中定义。

进入注释4：独立性可以通过对所审核活动的责任自由或对偏见和利益冲突的自由来证明。

3.19
测量
*过程*确定一个值

3.20
监控
确定系统，*流程*或活动的状态

注释1：要确定状态，可能需要检查，监督或严格观察。

3.21
理事机构
对*组织的*活动，治理和*政策*负有最终责任和权力，并且*最高管理者*向其报告并由最高管理者负责的个人或一群人

注释1：并非所有组织，特别是小型组织，都将拥有一个独立于高层管理人员的理事机构。

注释2：理事机构可以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
在国家法律或惯例中被视为工作关系的关系中的个人，或在依赖于组织活动的合同关系中的*个人*

3.23
合规功能
对遵从性管理系统的运作 *负有责任和权限的个人或团体*

注释1：最好将一个人分配给合规管理系统的监督。

3.24
合规风险
*不*遵守与组织*遵守 义务 发生的 可能性和后果*

3.25
合规义务
组织（SI）*强制 必须*遵守的*要求*以及组织自愿选择遵守的要求

3.26
遵守
满足*组织的*所有*要求 合规义务*

3.27
违规
未履行*履约义务*

3.28
合规文化
遍布整个*组织*的价值观，道德，信念和*行为*，并与组织的结构和控制系统进行交互以产生有助于*合规*的行为规范

3.29
执行
影响客户，员工，供应商，市场和社区成果的行为和做法

3.30
第三方
独立于组织的个人或机构

注释1：所有业务伙伴均为第三方，但并非所有第三方均为业务伙伴。

3.31
程序
指定的进行活动或过程的方式

[来源：ISO 9000：2015，3.4.5]

4 组织环境

4.1 了解组织及其背景

组织应确定与其目的相关并影响其实现合规管理系统预期结果能力的外部和内部问题。

为此，组织应考虑广泛的问题，包括但不限于：

— 业务模型，包括战略，性质，规模和规模的复杂性以及组织活动和运营的可持续性；

— 与第三方的业务关系的性质和范围；

— 法律和法规环境；

— 经济状况；

— 社会，文化和环境背景；

— 内部结构，政策，流程，程序和资源，包括技术；

— 它的合规文化。

4.2 了解有关方面的需求和期望

组织应确定：

— 与合规管理系统有关的利害关系方；

— 这些利害关系方的有关要求；

— 这些要求中的哪些将通过合规管理系统解决。

4.3 确定合规管理系统的范围

组织应确定合规管理系统的范围和适用性以建立其范围。

注：合规管理系统的范围旨在阐明组织面临的主要合规风险以及合规管理系统将适用的地理或组织边界，或两者都适用，特别是在组织是大型实体的一部分的情况下。

在确定此范围时，组织应考虑：

— 4.1中提到的外部和内部问题；

— 4.2、4.5 和4.6中提到的要求。

该范围应作为文档信息提供。

4.4 合规管理系统

组织应根据本文件的要求建立，实施，维护和持续改进合规管理系统，包括所需的过程及其相互作用。

遵从管理体系应反映组织的价值观，目标，战略和遵从风险，并考虑到组织的环境（见4d）。

4.5 合规义务

组织应系统地识别其活动，产品和服务产生的合规义务，并评估其对运营的影响。

组织应具备以下流程：

a) 确定新的和更改的合规义务，以确保持续合规；

b) 评估已识别变更的影响，并在合规义务管理中实施任何必要的变更。

组织应保持其合规义务的书面信息。

4.6 合规风险评估

组织应基于合规风险评估，识别，分析和评估其合规风险。

组织应通过将合规义务与其活动，产品，服务和运营的相关方面相关联来识别合规风险。

组织应评估与外包和第三方流程相关的合规风险。

应定期评估合规风险，并应在情况或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以及应对其合规风险的措施的书面信息。

5 领导

5.1 领导与承诺

5.1.1 领导机构和高层管理人员

理事机构和最高管理者应通过以下方式表现出对合规管理体系的领导和承诺：

— 确保建立合规政策和合规目标并与组织的战略方向兼容；

— 确保将合规管理系统要求集成到组织的业务流程中；

— 确保合规管理系统所需的资源可用；

一传达有效的合规管理和遵守合规管理系统要求的重要性；

— 确保合规管理系统达到预期结果；

－指导和支持人员为合规管理系统的有效性做出贡献；

— 促进持续改进；

— 支持其他相关角色以展示其在其职责范围内的领导能力。

注意：本文档中对“业务”的引用可以广义地解释为那些对于组织存在的目的而言至关重要的活动。

理事机构和最高管理者应：

— 建立并维护组织的价值观；

— 确保制定和实施政策，流程和程序以实现合规目标；

— 确保及时告知他们有关合规事宜，包括不合规的情况，并确保采取适当的措施；

— 确保遵守承诺，并适当处理违规和违规行为；

— 确保适当地将合规责任包括在职位描述中；

— 任命或提名合规职能；

— 确保按照2x3提出和解决问题的系统。成立。

5.1.2 合规文化

组织应在组织内的各个层次上建立，维护和促进合规文化。

理事机构，高层管理人员和管理层应表现出对整个组织所需的共同行为和行为标准的积极，可见，一致和持续的承诺。

最高管理者应鼓励建立和支持合规的行为。它应防止而不是容忍损害合规性的行为。

5.1.3 合规治理

理事机构和最高管理者应确保执行以下原则：

— 直接将遵约职能移交给理事机构；

— 遵守职能的独立性；

— 合规职能的适当权限和能力。

注1：直接访问可包括：直接向理事机构报告，向理事机构定期提交报告并参加其会议。

注2：独立是指对顺应功能的操作没有任何不适当的干扰或压力，或两者都不存在。

5.2 合规政策

理事机构和最高管理者应制定合规政策，以：

a) 适合组织的目的；

b) 提供设定合规目标的框架；

c) 包括满足适用要求的承诺；

d) 包括对合规管理系统的持续改进的承诺。

遵守政策应：

— 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；

— 支持符合5.1.3的合规性治理原则：

— 参考并描述合规功能；

— 概述不遵守组织的合规义务，政策，流程和程序的后果；

— 鼓励引起关注并禁止任何形式的报复；

— 用通俗易懂的语言写成，以便所有人员都可以轻松理解其原理和意图；

— 适当实施和执行；

— 可以作为记录信息使用；

— 在组织内部进行沟通；

— 适当时可供感兴趣的各方使用。

5.3 角色，职责和权限

5.3.1 领导机构和高层管理人员

理事机构和最高管理者应确保在组织内分配和传达有关角色的职责和权限。

理事机构和最高管理者应分配以下职责和权限：

a) 确保合规管理系统符合本文件的要求；

b) 向理事机构和最高管理者汇报合规管理系统的绩效。

理事机构应：

— 确保根据达到合规目标衡量最高管理层；

－对最高管理者进行有关合规性管理系统运行的监督。

最高管理者应：

— 分配足够和适当的资源以建立，开发，实施，评估，维护和改进合规管理系统；

一确保建立有效的及时报告履约情况的系统；

— 确保战略和运营目标与合规义务之间保持一致；

— 建立和维护问责机制，包括纪律处分和后果；

— 确保将合规绩效纳入人员绩效评估。

5.3.2 合规功能

合规职能应负责合规管理系统的运行，包括以下内容：

— 促进确定履约义务；

— 记录合规风险评估；

— 使合规管理系统与合规目标保持一致；

— 监控和衡量合规绩效；

— 分析和评估合规性管理系统的性能，以确定是否需要采取纠正措施；

— 建立合规报告和文件记录系统；

— 确保按计划的时间间隔审核合规性管理系统（请参阅*92* 和9.3）：

— 建立引起关注并确保解决关注的系统。

遵守职能应监督：

— 在整个组织中适当分配实现已确定合规性义务的职责；

— 合规义务已整合到政策，流程和程序中；

— 所有相关人员均按要求接受培训；

— 建立合规绩效指标。

遵从功能应提供：

— 有权访问合规政策，流程和程序资源的人员；

— 就合规性相关事宜向组织提供建议。

注意合规功能的特定职责并不能免除其他人员的合规责任。

组织应确保符合性功能可以访问：

— 高级决策者，以及在决策过程中尽早做出贡献的机会；

— 组织的各个级别；

— 所需的所有人员，文件化信息和数据；

—有关有关法律，法规，守则和组织标准的专家意见。

5.3.3 管理

管理层应通过以下方式负责其职责范围内的合规：

— 与合规部门合作并提供支持，并鼓励人员这样做；

— 确保其控制范围内的所有人员均遵守组织的合规义务，政策，流程和程序；

—识别并传达其运营中的合规风险；

— 将合规义务纳入其职责范围内的现有业务实践和程序中；

— 参加和支持合规培训活动；

— 培养人员对合规义务的意识，并指导他们满足培训和能力要求；

— 鼓励其人员提出合规性问题并给予支持，并排除任何形式的报复行为；

— 根据需要积极参与管理和解决与合规性相关的事件和问题；

— 确保在确定需要采取纠正措施后，建议并实施适当的纠正措施。

5.3.4 人员

所有人员应：

— 遵守组织的合规义务，政策，流程和程序；

— 报告合规问题，问题和失败；

— 参加所需的培训。

6 规划

6.1 应对风险和机遇的行动

在规划合规管理系统时，组织应考虑4JL中提到的问题和*4* ^ *2*
中提到的要求，并确定需要解决的风险和机遇：

— 确保合规管理系统可以达到预期结果；

— 防止或减少不良影响；

— 实现持续改进。

在规划合规管理系统时，组织应考虑：

— 其合规目标（见^ 2）；

— 确定的合规义务（请参阅4.5）：

— 合规风险评估的结果（见4.6）。

组织应计划：

a) 应对这些风险和机遇的行动；

b) 如何：

1) 将行动整合并实施到其合规管理系统流程中；

2) 评估这些措施的有效性。

6.2 合规目标和实现目标的计划

组织应在相关职能和级别上建立合规目标。

遵守目标应：

a) 与合规政策保持一致；

b) 可衡量的（如果可行）；

c) 考虑适用的要求；

d) 被监视；

e) 沟通；

f) 适当更新；

g) 作为文档信息可用。

在计划如何实现其合规目标时，组织应确定：

— 将要做什么；

— 需要什么资源；

— 谁来负责；

— 何时完成；

— 如何评估结果。

6.3 变更计划

当组织确定需要更改合规管理系统时，应以计划的方式进行更改。

组织应考虑：

— 变更的目的及其潜在后果；

— 合规管理系统的设计和运营有效性；

— 是否有足够的资源；

— 职责和权限的分配或重新分配。

7支持

7.1 资源

组织应确定并提供建立，实施，维护和持续改进合规管理系统所需的资源。

7.2 权限

7.2.1 一般的

组织应：

—确定在其控制下从事影响其合规表现的人员的必要能力；

-根据适当的教育，培训或经验，确保这些人胜任；

—在适用的情况下，采取行动以获得必要的能力，并评估所采取行动的有效性。

应提供适当的书面信息作为胜任力的证据。

注：可采取的行动包括，例如，提供培训，指导或重新安排在职人员；或雇用或签约合资格的人。

7.2.2 就业过程

就其所有人员而言，组织应制定，建立，实施和维护流程，以使：

a) 雇用条件要求人员遵守组织的合规义务，政策，流程和程序；

b) 在开始雇用的合理期间内，员工将收到遵从政策的副本或对其进行访问并获得有关该政策的培训的机会；

c) 对于违反组织合规性义务，政策，过程和程序的人员，应采取适当的纪律处分。

作为雇用过程的一部分，组织应考虑由角色和人员造成的合规风险，并在雇用，调动和晋升之前按照要求进行尽职调查程序。

组织应实施一个程序，对绩效目标，绩效奖金和其他激励措施进行定期审查，以验证是否已采取适当的措施来防止鼓励违规行为。

7.2.3 训练

组织应从雇用开始之时起，并按组织确定的计划间隔定期对有关人员进行培训。

培训应为：

a) 适合人员的角色以及人员所面临的合规风险；

b) 评估有效性；

c) 定期审查。

考虑到已识别的合规风险，组织应确保实施程序以解决对合规意识的培训，以及对代表其行事并可能给组织带来合规风险的第三方的培训。

培训记录应保留为书面信息。

7.3 意识

在组织控制下工作的人员应了解：

— 遵守政策；

— 它们对合规管理系统有效性的贡献，包括改进合规绩效的好处；

— 不符合合规管理系统要求的影响；

— 引起合规性问题的程序和程序的方式（见S3）；

— 遵守政策与其职责相关的遵守义务的关系；

— 支持合规文化的重要性。

7.4 沟通

组织应确定与合规管理系统有关的内部和外部通信，包括：

a) 关于它将传达什么；

b) 何时沟通；

c) 与之沟通；

d) 如何沟通。

组织应：

— 在考虑其传播需求时，考虑多样性的方面和潜在的障碍；

— 确保在建立其沟通流程时考虑到有关方面的意见fes）；

— 建立沟通流程时）：

  — 包括关于其合规文化，合规目标和义务的沟通；

  — 确保要传达的合规信息与合规管理系统内生成的信息一致并且可靠；

一回应有关其合规管理系统的相关沟通；

— 适当保留文件化信息作为其通讯的证据；

— 在组织的各个级别和职能之间内部传达与合规管理系统有关的信息，包括酌情更改合规管理系统；

— 确保其沟通过程使人员能够为持续改进合规管理系统做出贡献；

— 确保其沟通过程使人员能够提出疑虑（见S3）；

— 由组织的沟通流程建立的外部沟通与合规管理系统有关的信息，并包括有关其合规文化，合规目标和义务的交流。

7.5 记录的信息

7.5.1 一般的

组织的合规管理系统应包括：

a) 本文件要求的文件资料；

b) 组织确定为达标管理系统的有效性所必需的文件化信息。

注：遵从性管理系统的文档化信息范围可能因一个组织而异，这是由于以下原因：

— 组织的规模及其活动，过程，产品和服务的类型；

— 流程及其交互的复杂性；

— 人的能力。

7.5.2 创建和更新文档信息

在创建和更新文档信息时，组织应确保适当：

— 标识和描述（例如标题，日期，作者或参考编号）；

— 格式（例如语言，软件版本，图形）和媒体（例如纸张；电子）；

— 审查和批准其适用性和适当性。

7.5.3 控制文件信息

合规管理系统和本文件所要求的文件信息应受到控制，以确保：

a) 它是可用的，并且适合在需要的地方和时间使用；

b) 它得到了充分的保护（例如，避免了机密性，使用不当或完整性的损失）。

为了控制书面信息，组织应酌情开展以下活动：

— 分发，获取，检索和使用；

— 储存和保存，包括保持易读性；

— 控制变更（例如版本控制）；

— 保留和处置。

组织应确定必要的外部来源的书面信息，这些信息对于合规性管理系统的计划和运行是必要的，并应加以控制。

注意访问可能意味着要决定是否仅允许查看文档信息，或者是有关查看和更改文档信息的权限。

8 运行

8.1 运行计划与控制

组织应通过以下方式计划，实施和控制满足要求所需的过程，以及实施第6条 中确定的措施：

— 建立过程标准；

— 根据标准实施过程控制。

应提供必要的书面信息，以确信该过程已按计划进行。

组织应控制计划的变更并审查意外变更的后果，并采取必要的措施以减轻任何不利影响。

组织应确保控制与合规管理系统相关的外部提供的过程，产品或服务。

注意：将组织的业务外包不会减轻组织的法律责任或合规性义务。

组织应确保对第三方过程进行控制和监视。

8.2 建立控制和程序

组织应实施控制措施以管理其合规义务和相关的合规风险。这些控制措施应予以维护，定期检查和测试，以确保其持续有效性。

注：测试控件是指进行有计划的练习，以查看控件是否达到了预期的目的或不能被绕过，或者在降低风险的影响或可能性方面是否有效。

8.3 引起关注

组织应建立，实施和维护一个过程，以鼓励和报告（在合理的理由下认为该信息是真实的）企图，怀疑或实际违反合规政策或合规义务的情况。

该过程应：

— 在整个组织中可见并可以访问；

— 保密地处理报告；

— 接受匿名举报；

— 保护举报人免受报复；

— 使人员能够接收建议。

组织应确保所有人员都了解报告程序，其权利和保护并能够使用它们。

8.4 调查程序

组织应制定，建立，实施和维护过程，以评估，评估，调查和结清关于可疑或实际违规事件的报告。这些程序应确保公平公正的决策。

调查过程应由主管人员独立进行，不得有利益冲突。

组织应将调查结果用于适当地改进合规管理系统（参见第10条）。

组织应定期向理事机构或最高管理者报告调查的数量和结果。

组织应保留有关调查的书面信息。

9 绩效评估

9.1 监测，测量，分析和评估

9.1.1 总则

组织应监视合规管理系统，以确保实现合规目标。

组织应确定：

— 需要监视和测量的内容；

— 为确保有效结果而进行的监测，测量，分析和评估方法；

一，何时进行监测和测量；

— 监测和测量的结果应进行分析和评估。

文件信息应作为结果的证据。

组织应评估合规绩效和合规管理系统的有效性。

9.1.2 有关合规绩效的反馈来源

组织应建立，实施，评估和维护过程，以从各种来源寻求并接收有关其合规绩效的反馈。应对信息进行分析和严格评估，以找出不符合项的根本原因，确保采取适当的措施，并将此信息反映在 生6·要求的定期风险评估中

9.1.3 指标制定

组织应制定，实施和维护一套适当的指标，以帮助组织评估其合规目标的实现并评估其合规绩效。

9.1.4 合规报告

组织应建立，实施和维护合规报告流程，以确保：

a) 确定了适当的报告标准；

b) 确定定期报告的时间表；

c) 实施了例外报告系统，以促进临时报告；

d) 实施系统和流程以确保信息的准确性和完整性；

e) 向组织的正确职能或领域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。

合规部门向理事机构或最高管理层发布的任何报告均应得到充分保护，以免发生变更。

9.1.5 保持记录中

必须保留组织合规活动的准确，最新记录，以帮助进行监视和审查过程，并证明与合规管理系统的符合性。

9.2内部审核

9.2.1 总则

组织应按计划的时间间隔进行内部审核，以提供有关合规管理系统是否：

a) 符合：

— 组织对合规管理系统的要求；

— 本文件的要求；

b) 有效地实施和维护。

9.2.2 内部审核程序

组织应计划，建立，实施和维护审核计划，包括频率，方法，职责，计划要求和报告。

在建立内部审核计划^）时，组织应考虑相关过程的重要性以及以前审核的结果。

组织应：

a) 确定每次审核的审核目标，标准和范围；

b) 选择审核员并进行审核，以确保审核过程的客观性和公正性；

c) 确保将审核结果报告给相关管理人员和管理层。

注1：相关管理可以包括合规职能，最高管理者和管理机构。

应提供书面信息，作为审核计划和审核结果实施的证据。

注2：ISO 19011中给出了有关审核管理系统的指南。

9.3 管理评审

9.3.1总则

领导机构和最高管理者应按计划的时间间隔审查组织的合规管理系统，以确保其持续的适用性，充分性和有效性。

9.3.2 管理评审输入

管理评审应包括：

a) 先前的管理评审所采取的措施的状态；

b) 与合规管理系统相关的外部和内部问题的更改；

c) 与合规管理系统有关的利害关系方的需求和期望的变化；

d) 有关合规绩效的信息，包括以下方面的趋势：

—不合格，不合规和纠正措施；

—监测和测量结果；

-审计结果；

e) 持续改进的机会。

管理评审应考虑：

— 遵守政策的充分性；

— 遵守职能的独立性；

— 达到合规目标的程度；

— 资源是否充足；

— 合规风险评估的充分性；

— 现有控制措施和绩效指标的有效性；

— 提出疑虑的人，有关方面的沟通，包括反馈（见9.1.2）和投诉；

-调查（见脂）；

— 报告系统的有效性。

9.3.3 管理评审结果

管理评审的结果应包括与持续改进机会以及对合规管理体系进行任何更改的需求有关的决策。

应提供书面信息，作为管理评审结果的证据。

10 改进

10.1持续改进

组织应不断提高合规管理体系的适用性，充分性和有效性。

10.2 不合格和纠正措施

当发生不符合项或不符合项时，组织应：

a) 对不符合项或不符合项做出反应，并在适用的情况下：

1) 采取措施进行控制和纠正；

2) 处理后果；

b) 评估采取行动消除不合格或不合规原因或两者的原因的必要性，以使其不会在其他地方再次发生或发生，方法是：

1) 审查不合格或不合规，或两者兼而有之；

2) 确定不合格或不合格或两者的原因；

3) 确定是否存在相似的不合格品或不合格品，或同时存在或可能发生类似的不合格品；

c) 实施所需的任何行动；

d) 审查采取的任何纠正措施的有效性；

e) 如有必要，对合规性管理系统进行更改。

纠正措施应适合于所遇到的不合格或不合格或两者的影响。

应提供书面信息作为以下方面的证据：

— 不符合或不符合或两者的性质，以及随后采取的任何措施；

— 任何纠正措施的结果。

附件A
（资料性的）

本文件使用指南

A.l背景和范围

A.1.1总则

本附件中指南的目的是指出组织在实施合规性管理系统时可以采取的方法和行动类型。它并不旨在是全面的或规范性的，组织也没有义务实施本指南中的所有建议以使合规性管理系统满足本文档的要求。为了履行其合规义务，组织应就其合规风险的性质和范围采取合理的措施。

组织可以选择将此遵从性管理系统作为一个单独的系统来实施，但是，理想情况下，它将与其他管理系统（例如风险，反贿赂，质量，环境，信息安全和社会责任）一起实施。举几个例子。在这种情况下，组织可以参考ISO 31000，ISO 37001，ISO 9001，ISO 14001和ISO / IEC 27001以及ISO 26000。

A.1.2范围

任何规模，复杂性或行业的组织都可以按照其要求将本文档应用于创建合规性管理系统。这将使他们了解其背景，业务运营，由此产生的义务和合规风险，并帮助他们采取合理的步骤来履行其义务。应遵守文件中的每个要求。但是，仅推荐本附件中的指南。

实际上，在小型组织中，根据本文档实施合规性管理系统通常较为容易，因为它们不那么复杂。中小型组织将通过使用本文档要求的原则来增强其组织实践。

本文档涉及理事机构和高层管理人员，并定义了这些术语在各种上下文和位置中的含义。本文档可供所有组织使用，因此，如果特定组织不使用这些术语，请注意其使用意图：要求或指示将适用于在顶峰拥有权威和责任的个人或人群组织的。

A.2规范性引用文件

本文档无规范性引用。用户可以参考参考书目以获取与合规性相关的其他信息和国际标准。

A.3术语和定义

该文件采用了ISO开发的高级结构（HLS），以改善其国际管理体系标准之间的一致性。HLS结构列出了子句序列，通用术语和定义，以及构成ISO管理系统标准（MSS）核心的相同核心文本。这意味着某些定义可以以不熟悉的方式使用。提供的定义可以在使用本文档时提供澄清。

MSS的这种通用方法为用户增加了此类标准的价值。对于选择运行可以同时满足两个或多个MSS要求的单个（有时称为“集成”）管理系统的组织而言，此功能特别有用。尚未采用MSS或合规性管理框架的组织可以轻松地将此文档作为其组织内的独立指南。

有关MSS和HLS结构的更多信息，请访问：https：//www.iso.o ） g / management · system-standards.html。

A.4组织的背景

A.4.1了解组织及其背景

该条款的目的是组织对可能影响其合规性管理系统的重要问题建立高层（例如战略）理解。然后，所获得的知识将用于指导规划，实施，操作和改进合规性管理系统的方法。

这是审查有关组织的所有可用信息的过程：组织做什么，在哪里，如何以及为什么。根据合规义务评估外部和关键因素对组织的影响。

这些合规性义务中最明显的是组织在其经营所在的法律和法规环境中产生的，但义务或风险也可能由本文档中建议的其他因素引起。组织还应考虑可能会产生影响的相关未来趋势。

应考虑内部因素。文档中包含一些示例。此列表并不详尽，并且可能还有其他与组织相关的列表。

A.4.2了解有关方面的需求和期望

组织应建立对可能会影响合规管理系统，受其影响或认为自己受到合规管理系统影响的人员或组织的需求和期望的理解。

有些是强制性的，因为它们已被纳入正式的要求中，例如法律，法规，许可证和执照以及政府或法院的诉讼。可能存在此处未包括的其他正式要求。

当指定了利益相关方的其他需求和期望时，这些义务和义务就成为了义务，并且组织决定通过签订协议或合同自愿采用这些义务和期望。一旦组织决定了它们，它们便成为合规义务。

外部利益相关方的示例包括：

— 政府和政府机构；

监管机构；

-顾客;

-承包商；

—供应商；

-第三方中介；

— 所有者，股东和投资者；

非政府组织；

— 社会和社区团体；

-商务伙伴。

内部利益相关方的示例包括：

— 理事机构；

-管理;

-雇员;

— 内部职能，例如风险管理，内部控制，内部审计，人力资源。

A.4.3确定合规管理体系的范围

确定遵从性管理系统的范围是组织确定遵从性管理系统将应用到的物理和组织边界的过程。这样，组织可以自由选择在整个组织内，组织中的特定单位或特定职能中实施法规遵从管理系统的自由度和灵活性。

通常，合规管理系统将在整个组织中实施，对于一组组织而言，则将在整个组织中实施，以避免道德行为和合规的双重标准。

考虑到组织所面临的合规风险的性质和程度，范围应合理且相称。

建立合规管理系统的范围并确定组织将采用哪些要求时，应考虑对相关利益方的上下文和要求的了解。

A.4.4合规管理体系

合规管理系统是一个框架，该框架集成了必要的结构，政策，流程和程序，以实现所需的合规结果，并采取措施防止，发现和应对不合规情况。

通常，合规性管理系统框架是结构性问题：构建该系统所必需的基础结构。然后需要通过执行政策，流程和程序来使其可操作。然后，需要对其进行维护并对其进行持续改进。

合规性管理系统包含许多要素。管理系统的某些元素将被设计为支持所需的行为，而其他元素将被设计为防止不良行为。有些元素仅用于监视组织的合规性绩效，或者在发生不合规情况时发出警报。

合规管理系统将认识到确实会发生错误，并将制定流程以确保做出适当的反应。适当的反应将包括对流程，系统和受影响方的补救。

遵守管理系统应基于善政，相称性，完整性，透明度，问责制和可持续性的原则。

合规管理系统应作为文档信息提供。

A.4.5合规义务

组织应将合规义务作为建立，开发，实施，评估，维护和改进其合规管理体系的基础。

组织强制性必须遵守的要求包括：

— 法律法规；

— 许可证，执照或其他形式的授权；

— 监管机构发布的命令，规则或指南；

— 法院或行政法庭的判决；

— 条约，公约和议定书。

组织自愿选择遵守的要求可以包括：

— 与社区团体或非政府组织的协议；

— 与公共机构和客户的协议；

— 组织要求，例如政策和程序；

— 自愿性原则或行为准则；

— 自愿标签或环境承诺；

— 与组织的合同安排下产生的义务；

— 相关的组织和行业标准。

组织应按部门，职能和组织活动的不同类型确定合规义务，以确定谁受这些合规义务影响。

获取有关法律变更和其他合规义务的信息的过程可以包括：

— 在相关监管机构的邮件列表中；

一，专业团体的成员；

— 订阅相关的信息服务；

— 参加行业论坛和研讨会；

— 监控监管机构的网站；

— 与监管机构会面；

— 与法律顾问的安排；

-监视合规义务的来源（例如，法规声明，法院判决）。

应该采取基于风险的方法，即组织应首先确定与业务相关的最重要的合规义务，然后集中精力处理所有其他合规义务（帕累托原理）。

在适当的情况下，组织应建立并维护一个列出所有合规义务的文件（例如注册簿或日志），并制定一个定期更新该文件的过程。

除规定合规义务外，该文件还应包括但不限于：

— 履约义务的影响；

— 遵守义务的管理；

— 与合规义务相关的控制；

-风险评估。

A.4.6合规风险评估

合规风险评估是实施合规管理系统以及分配适当和足够的资源和流程以管理已识别合规风险的基础。

合规风险的特征是发生的可能性以及不遵守组织的合规政策和义务的后果。

合规风险包括固有合规风险和残留合规风险。固有合规风险是指组织处于不受控制的状态而没有任何相应的合规风险处理措施时所面临的所有合规风险。残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。

组织应通过考虑违规的根本原因和根源以及后果，来分析合规风险，同时包括可能发生这些后果的可能性。后果可以包括例如人身和环境损害，经济损失，名誉损害，行政变更以及民事和刑事责任。

合规风险的标识包括合规风险源的标识和合规风险情况的定义。组织应根据部门职责，职务职责和不同类型的组织活动，识别各个部门，职能和不同类型的组织活动中的合规风险源。组织应定期识别合规风险源，并定义与每个合规风险源相对应的合规风险情况，以制定合规风险源列表和合规风险情况列表。

风险评估包括将组织可以接受的合规风险水平与合规政策中规定的合规风险水平进行比较。

应定期评估合规风险，并在存在以下情况时重新评估合规风险：

— 新的或更改的活动，产品或服务；

— 改变组织的结构或策略；

-重大的外部变化，例如财务经济状况，市场状况，负债和客户关系；

— 变更合规义务；

— 并购；

— 不合规（即使是单个不合规事件也可能构成情况的重大变化）和差错。

合规风险评估的详细程度和水平取决于组织的风险状况，背景，规模和目标，并且对于特定的子领域（例如环境，财务，社会）可能有所不同。

基于风险的合规管理方法并不意味着对于低合规风险情况，组织可以接受不合规的情况。它可以帮助组织将主要注意力和资源集中在较高风险上，并将其作为优先事项，并最终覆盖所有合规风险。所有确定的合规风险/情况都将受到监控和处理。

进行风险评估时（请参见ISO 31000），应注意适当的技术（如IEC 31010中所述）。

A.5领导力

A.5.1领导和承诺

A.5.1.1领导机构和最高管理者

有效的合规性需要领导机构和遍布整个组织的最高管理层的积极承诺。

对于合规管理系统而言，至关重要的是，领导机构和高层管理人员必须清晰，可见地展示其对实现合规管理系统目标的承诺。

不合规可能会对业务造成负面影响，例如声誉受损，经营许可丧失，机会丧失以及大量成本。因此，理事机构和最高管理者应认识到有效合规管理的战略重要性。

该文件列出了领导者可以展示其承诺的多种方式。最基本的方法是通过积极可见的支持来建立和维护合规性管理系统。

承诺程度由以下程度指示：

— 理事机构和各级管理层积极表现出对通过其行动和决定建立，发展，实施，评估，维持和改进有效和响应迅速的合规管理系统的承诺；

— 合规政策由理事机构正式批准；

— 最高管理者负责确保充分实现对组织合规性的承诺；

— 各级管理人员始终向员工传达清晰的信息（以言语和行为表示），表明该组织将履行其合规义务；

— 在行动支持的清晰和令人信服的声明中，已向所有人员和有关各方广泛传达了合规承诺；

-合规职能的人员具有适当的能力，地位权限和独立性，这反映了有效合规的重要性，并可以直接与理事机构接触；

一
通过提高认识的活动和对所有人员和有关方面的培训，为建立，发展，实施，评估，维持和改善健全的合规文化分配了足够的资源；

— 政策，流程和程序不仅反映了法律要求，还反映了自愿守则和组织的核心价值；

— 组织为组织的各个级别分配并要求对遵从管理负责；

—对合规管理系统进行定期审查（建议至少每年一次）；

— 组织的合规绩效不断提高；

— 及时采取纠正措施；

— 理事机构和最高管理层正在遵循组织的合规性管理系统。

A.5.1.2合规文化

支持合规文化发展的因素可以包括：

— 清晰的公开价值集；

— 积极，明显地执行和遵守价值观的管理；

— 在不遵守规定的情况下保持一致，无论其职位如何；

— 以身作则的指导，指导和领导；

— 对潜在人员进行关键职能（包括尽职调查）的适当的职前评估；

— 强调合规性和组织价值观的入职培训或入职培训；

— 持续的合规培训，包括对所有人员和有关方面的培训的更新；

— 持续就合规问题进行沟通；

— 考核考核制度，该考核制度应考虑对合规行为的评估并考虑绩效薪酬，以实现合规关键绩效指标和成果；

— 对合规管理成就和成果的可见认可；

— 在故意或过失违反合规义务的情况下，迅速而按比例地进行纪律处分；

— 组织战略与个人角色之间的明确联系，强调合规性对于实现组织成果至关重要；

— 在内部和外部进行有关合规性的公开且适当的沟通。

遵守文化的证据由以下程度指示：

— 以上各项已执行；

— 有关各方（特别是人员）认为上述各项已得到执行；

— 人员了解与他们自己的活动和其业务部门的活动相关的合规义务的相关性；

— 解决不合规问题的纠正措施是“拥有的”，并根据需要在组织的所有适当级别上采取措施；

— 遵守职能的作用及其目标得到重视；

— 鼓励并鼓励员工向合规管理人员提出合规问题，包括高层管理人员和理事机构。

该组织应：

a) 衡量其合规文化；

b) 征求所有人员的意见，以确定他们是否理解理事机构，高层管理人员和中层管理人员对合规的承诺；

c) 根据组织的合规文化指标的结果制定行动计划。

A.5.1.3合规治理

合规治理基于以下基本原则。

合规职能可直接与理事机构和高层管理人员联系。他们可以绕过组织中的其他人员（如果有必要），并直接与最有权采取行动的人员进行沟通。这对理事机构和高层管理人员有直接好处，因此他们可以行使职责。这种访问应该经过计划和系统的。例如，合规部门可以直接向首席执行官报告，向审计委员会，主席或整个董事会报告“虚线”。

合规职能应该是独立的，并且不应与组织结构或其他要素相冲突。他们可以自由采取行动，而不受生产线管理的干扰。

遵从功能具有权限。合规职能不是可以被推翻的初级职位，也不可以由权限较高的人员更改报告或信息。合规职能可以根据需要指导其他人员。合规职能部门应该有一个“ Mvoice”，以倡导并提出任何合规问题。

合规职能有足够的资源来支持组织不受限制地执行合规管理系统的必要工作和职责，包括获得技术以使合规管理系统能够全面有效地支持组织实现其合规目标。

A.5.2遵从政策

遵从政策建立了组织的总体原则和行动承诺，以实现组织的遵从。它确定了所需的责任和绩效水平，并确定了将要评估的行动的期望。该策略应适合组织因其活动而产生的合规义务。

合规政策应由理事机构批准。

合规政策应指定：

— 与组织及其运营环境的规模，性质和复杂性相关的合规性管理系统的应用程序和上下文；

— 合规程度将与治理，风险，审计和法律等其他职能整合的程度；

— 与内部和外部利益相关方的关系将得到管理的原则。

合规政策不应是独立的文档，而应得到其他文档的支持，包括运营策略和流程。

如有必要，应将合规政策翻译成其他语言。

合规政策应适合因组织范围和活动而产生的合规义务。

在制定合规政策时，应考虑：

a) 具体的国际，区域或地方义务；

b) 组织的战略，目标，文化和治理方法；

c) 组织的结构；

d) 与违规有关的风险的性质和水平；

e) 通过的标准，规范，内部政策和程序；

f) 行业标准。

遵从策略可以包括：

— 任务说明；

— 一般政策声明；

— 管理策略以及职责和资源的分配；

— 标准遵守程序；

— 审核，尽职调查和合规性。

A.5.3角色，职责和权限

A.5.3.1领导机构和最高管理者

理事机构的积极参与和监督是有效合规管理系统不可或缺的一部分。这有助于确保人员充分了解组织的合规政策和运营合规程序，以及如何将其应用到他们的工作中，并确保他们有效地履行合规义务。

为了使合规管理系统有效，管理机构和最高管理者需要以身作则，坚持并积极，可见地支持合规和合规管理系统。

尽管规模不限其他组织或职能（包括现有委员会，组织单位）或将要素外包给合规专家，但许多组织还取决于其规模，由其全权负责合规管理。

最高管理者应鼓励建立和支持合规性的行为，并且不应容忍损害合规性的行为。

最高管理者应确保：

— 组织对遵守其价值观，目标和策略的承诺的一致性，以便适当地定位遵守情况；

— 鼓励所有员工接受实现自己负责或负责的合规目标的重要性；

— 建立鼓励举报违规行为的环境，举报员工可以免受报复；

— 将合规性纳入更广泛的组织文化和文化变革计划中；

— 识别违规行为并立即采取措施纠正或解决违规行为；

— 运营目标和目标不会损害合规行为。

最高管理者应参考KPI和其他关键信息按计划的时间间隔（例如每季度或每月一次）审查合规管理系统的性能，以确保合规管理系统实现其目标。

合规管理系统的有效性要求最高管理者通过制定标准和进行合理监督来作出承诺。最高管理者应了解合规管理系统的内容和操作，并应确保组织具有有效的合规管理系统的适当流程。

A.5.3.2遵从功能

许多组织都有专职人员（例如合规官）负责日常合规管理，有些组织有跨职能的合规委员会来协调整个组织内的合规。合规性功能与管理层一起工作。

并非所有组织都将创建离散的合规性功能。有些人会将此功能分配给现有职位或将该功能外包。外包时，组织应考虑不将整个合规性职能分配给第三方。即使将部分功能外包，它也应考虑对其保持授权并监督此类功能。

在分配合规性管理系统的责任时，应考虑确保合规性功能表明：

— 诚信和对合规的承诺；

— 有效的沟通和影响力技能；

一能够接受建议和指导的能力和地位;

— 在设计，实施和维护合规管理系统方面的相关能力；

— 自信，业务知识和经验以进行测试和挑战；

— 采取策略性，积极主动的合规方法；

— 有足够的时间来满足角色的需求。

合规职能应具有权力，地位和独立性。权威是指管理机构和最高管理者授予合规职能足够的权力。身份意味着其他人员可能会听取并尊重他/她的意见。独立性意味着合规职能尽可能不亲自参与面临合规风险的活动。

合规职能应没有利益冲突，以履行其职责。

A.5.3.3管理

最高管理者的职责不应被视为放弃其他级别的合规性管理，因为所有经理都应在合规性管理系统方面发挥作用。因此，重要的是清楚地阐明他们各自的职责并将其包括在他们的职务说明中。

经理的合规责任将根据权限级别，影响力和其他因素（例如组织的性质和规模）而有所不同。但是，某些职责可能在各种组织中是共同的。

A.5.3.4人员

所有人员均应遵守合规义务。

人员应确保他们了解自己的合规责任并有效地履行它们。为此，将通过合规管理系统的要素来为其提供支持，例如培训，政策和程序以及行为准则。

人员应积极主动地寻求见解和改进意见，以帮助遵守法规管理系统。

A.6规划

A.6.1应对风险和机遇的行动

遵从性管理系统的计划是在战略级别执行的，而运营计划则是针对运营计划和控制而制定的。

规划的目的是预测潜在的情况和后果，因此是预防性的。根据合规风险评估的结果，组织应计划如何在不良后果发生之前解决这些不良影响，以及如何从有利于支持合规管理体系有效性的有利条件或状

况中受益。

规划还应包括确定如何将被认为对合规管理系统必要或有益的行动纳入业务活动和流程。合并可以通过目标设定，运营控制或其他特定条款（例如资源规定，权限）来实现。还应该计划评估合规管理系统有效性的措施。这可以包括监视，度量技术，内部审核或管理评审。

A.6.2合规目标和实现这些目标的计划

应该以可以测量结果的方式指定目标。

合规目标的一个示例：至少每年对相关人员进行合规培训。

应该确定实现目标所需的行动（即“什么”），相关的时间范围（即“何时”）和负责人（即“谁”）。应根据需要定期监测，记录，评估和更新目标的状态和进度。

一种。7支持

A.7.1资源

资源包括财务，人力和技术资源，以及获得外部建议和专门技能，组织基础设施，专业发展，技术以及有关合规管理和法律义务的当代参考资料。

A.7.2能力

A.7.2.1总则

术语“能力”是指应用知识和技能以达到预期结果的能力。能力需要知识，经验和技能，以便人们可以有效地履行其职责。组织应为所有人员确定完成其任务所需的专业知识和知识，以便组织可以向客户提供其产品和服务。组织应建立胜任力的证据（例如工作说明，职位陈述），在填补职位时可以考虑这些证据。

应采取措施（例如培训）以确保维持现有能力并获得新能力。应该有足够的能力证明文件，以及为保持或获得这些能力而采取的措施。

A.7.2.2就业过程

在雇用人员或提拔现有人员之前，组织应进行尽职调查，包括参考或背景调查。

A.7.2.3培训

履行合规义务的理事机构，管理层和人员应有能力有效地履行这些义务。能力的实现可以通过多种方式实现，包括通过教育，培训或工作经验所需的技能和知识。

培训计划的目的是确保人员有能力以与组织的合规文化及其对合规承诺相一致的方式胜任其职务。

正确设计和执行的培训可以为工作人员提供有效的方式，以传达以前无法确定的合规风险。

教育和培训应：

— 在适当的情况下，基于对员工知识和能力差距的评估；

— 具有足够的灵活性以说明一系列技术，以适应组织和人员的不同需求；

— 由经验丰富且合格的人员设计，开发和交付；

— 以适用的当地语言提供；

— 定期评估和评估其有效性。

如果不遵守规定会导致严重后果，则交互式培训可能是最佳的培训形式。

组织应在发生不当行为的地区提供培训。

只要存在以下情况，就应考虑合规性再培训：

— 职位或职责的改变；

— 内部政策，流程和程序的变化；

— 组织结构的变化；

— 遵守义务的变化，尤其是法律要求和利害关系方的要求；

— 活动，产品或服务的变更；

一由监控，审计，审查，投诉和不合规引起的问题，包括有关方面的反馈。

A.7.3意识

意识涉及确保合规策略可供所有人员访问和使用，并被理解。

可以通过诸如但不限于以下方法来提高合规意识：

— 培训（面对面或在线）；

— 高层管理人员的沟通；

— 易于遵循且易于获取的参考资料；

— 定期更新合规性问题。

传达对合规性的承诺：

— 建立意识并激励人员采用合规管理系统；

— 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

应根据组织的政策，采用针对所有利益相关方的外部交流的实用方法。

感兴趣的各方可以包括监管机构，客户，承包商，供应商，投资者，紧急服务，非政府组织和邻居。

组织应分配适当的资源和具有相关知识的人员来协调和促进监管互动。

交流方法可以包括网站和电子邮件，新闻稿，广告和定期新闻通讯，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，参与社区活动和电话热线。这些方法可以鼓励理解和接受组织对合规性的承诺。

交流应遵循透明，适当，可信，响应，可访问和清晰的原则。

A.7.5文件信息

A.7.5.1总则

记录的信息可以包括：

— 组织的合规政策和程序；

— 合规管理系统的目标，指标，结构和内容；

— 分配角色和责任以实现合规性；

— 有关合规义务的登记册；

— 依从风险登记册，并根据依从风险评估流程确定治疗的优先级；

— 违规，未遂和调查的记录；

— 年度合规计划；

— 人事记录，包括但不限于培训记录；

— 审核过程，审核时间表和相关的审核记录。

文件化信息可以包括与监管报告要求有关的事项。记录的信息可以包括各种媒体（数字和非数字媒体）。

A.7.5.2创建和更新文档信息

应更新记录的信息以反映内部和外部的更改，以确保它们是最新的和最新的。

A.7.5.3文件信息的控制

可以准备文件化信息以获取法律建议，因此可以成为法律特权的主题。

A.8操作

A.8.1运作计划和控制

精心设计的合规性管理系统包括可以对合规文化既有内容又有影响的措施（例如政策，流程，程序）。他们着眼于减少合规风险评估过程中发现的风险，并旨在降低这些风险。

运营控制的基本要素是行为准则，其中规定了组织对相关合规性义务的完全承诺。行为准则应适用于所有人员，并可供他们使用。根据并源自行为准则，应将合规措施纳入组织的日常运营中，以培养合规文化。

与业务流程有关的情况需要操作控制，而缺少此类控制可能导致偏离合规政策或违反合规义务。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。

控制的程度可以根据几个因素而变化，例如所执行功能的重要性或复杂性，违规或涉及或可获得的技术支持的潜在后果。

当操作控制失败时，必须采取措施来解决任何不良后果。

如果组织的活动中使用了第三方或外包流程，则组织应进行有效的尽职调查，以确保不会降低其标准和对合规性的承诺。第三方的一个示例涉及产品和服务的提供以及产品的分销。组织应确保订立适当的服务水平协议（SLA），以规定服务提供商的合规义务。

精心设计的外包流程应考虑以下因素：

— 初步和正在进行的尽职调查；

— 实施适当的控制；

— 进行持续监控；

— 对法律/合同协议的适当审查；

— 审议SLA；

— 使用经本文档认证的第三方。

与第三方签订合同时，组织应实施控制措施，以确保对活动的采购，运营，商业和其他非财务方面进行适当的管理。根据组织和交易的规模，组织实施的采购，运营，商业和其他非财务控制措施可以降低合规风险。

A.8.2建立控制和程序

需要有效的控制措施以确保满足组织的合规义务，并防止，发现和纠正不合规情况。控件的设计应足够严格，以促进实现特定于组织活动和运营环境的合规性义务。此类控件应尽可能嵌入到正常的组织

过程中。

控件可以包括：

— 清晰，实用且易于遵循的书面操作政策，流程，程序和工作说明；

— 系统和异常报告；

-批准；

— 角色和职责不相容的隔离；

—自动化流程；

— 年度合规计划；

-人员绩效计划；

— 符合性评估和审核；

— 表现出管理承诺和模范行为；以及其他促进合规行为的措施；

— 就员工的预期行为（标准和价值观，行为准则）进行积极，公开和频繁的沟通。

在制定支持合规性管理的程序时，应考虑：

— 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；

一与组织中其他审查和控制职能的一致性；

— 持续的监测和测量；

— 评估和报告（包括管理监督）以确保员工遵守程序；

— 识别，报告和升级违规事件和违规风险的具体安排。

A.8.3提出关注

在适当的情况下，应将其升级至最高管理层和理事机构，包括有关委员会。

即使在当地法规没有要求的情况下，组织也应考虑建立举报人机制，以允许匿名或保密，以便组织的员工和代理商可以举报不合规行为或寻求指导，而不必担心受到报复。

有关举报管理系统的更多指南，请参见ISO 37002。

A.8.4调查过程

有效的合规管理系统的一个特点是一个运行良好的机制，用于及时，彻底地调查组织，其人员或相关第三方的任何指控或怀疑的不当行为。这包括组织响应的文档，包括所采取的任何纪律或补救措施，以及考虑到所汲取的教训对合规管理系统进行的修订。

一个有效的调查机制可以识别不当行为，合规管理系统漏洞和问责失误的根本原因，包括管理人员，高层管理人员和理事机构之间的关系。经过深思熟虑的根本原因分析可解决违规的程度和普遍性，所涉人员的数量和水平以及违规的严重性，持续时间和频率。

组织应确保调查是公正和独立的。他们应酌情考虑建立独立的委员会来监督调查并保证其完整性和独立性。

组织应建立有关调查的报告机制，包括报告调查结果的级别。

注意：法律有时会要求组织举报不合规情况。在这种情况下，将根据适用的法规或另行商定的方式通知监管部门。

即使法律没有要求组织举报不合规情况，也可以考虑将-
不合规情况自愿披露给监管机构，以减轻不合规的后果。

A.9绩效评估

A.9.1监测，测量，分析和评价

A.9.1.1概述

监视是收集信息的过程，目的是评估合规性管理系统和组织的合规性绩效的有效性。

对合规性管理系统的监视通常包括：

培训的有效性；

— 控制的有效性（例如通过样本测试输出）；

— 有效分配职责以履行合规义务；

— 履约义务的货币；

— 解决先前发现的合规性失败的有效性；

— 内部合规检查未按计划执行的情况；

— 针对合规风险审查业务策略，以进行适当的更新。

监视合规性能通常包括：

— 不遵守和“近乎失误”（即没有不良影响的事件）；

— 没有履行合规义务的情况；

— 达不到目标的情况；

— 遵守文化的状况；

— 建立领先和落后的指标。

A.9.1.2关于合规绩效的反馈来源

资料包括：

— 人员（例如通过举报设施，热线服务，反馈，建议箱）；

— 客户（例如通过投诉处理系统）；

－第三方；

—供应商；

-承包商；

-调节器；

— 过程控制日志和活动记录（包括基于计算机的和基于纸张的）。

关于合规性表现的反馈可以包括：

—合规性问题；

— 不合规和合规性问题；

— 新出现的合规问题；

— 持续的法规和组织变革；

— 关于合规有效性和绩效的评论。

有很多收集信息的方法。下面列出的每种方法在不同情况下都是相关的，应谨慎选择适合组织规模，规模，性质和复杂性的各种工具。

信息收集可以包括：

— 出现或发现不合规的临时报告；

— 通过热线电话，投诉和其他反馈（包括举报）获得的信息；

— 非正式讨论，讲习班和焦点小组；

— 抽样和完整性测试，例如神秘购物；

— 知觉调查的结果；

— 直接观察，正式采访，设施参观和检查；

— 审核和审查；

— 培训期间提供的有关方面的疑问，培训要求和反馈（尤其是员工的反馈）。

应该开发一个用于分类，存储和检索信息的系统。

信息管理系统应同时捕获问题和投诉，并允许对与合规性相关的问题进行分类和分析。分析应考虑系统性和反复出现的问题以进行纠正或改进，因为这些问题可能会给组织带来重大合规风险，并且可能更难以识别。

信息分类标准可以包括：

-来源;

-部门;

-不合规描述；

-义务参考；

— 指标;

严重程度；

— 实际或潜在影响。

A.9.1.3指标的制定

此过程应考虑合规风险的评估结果，以确保指标与组织的合规风险的相关特征相关。在什么方面以及如何衡量合规绩效的问题在某些方面可能具有挑战性，但仍然是证明合规管理系统有效性的重要组成部分。此外，所需的指标将随着组织的成熟度以及实施新的和修订的计划的时间和范围而变化。

指标可以包括：

一，受过有效培训的员工比例；

— 监管机构的联系频率；

— 反馈机制的使用情况（包括用户对这些机制的价值的评论）。

反应性指标可以包括：

— 确定的问题和不合规情况，按类型，面积和频率报告；

— 违规的后果，包括对金钱补偿，罚款和其他罚款，补救成本，声誉或员工成本*时间造成的影响进行评估；

— 报告和采取纠正措施所花费的时间。

预测指标可以包括：

— 不合规的风险衡量为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）；

— 不合规趋势（基于过去的趋势的预期合规率）。

A.9.1.4符合性报告

尽管报告系统性和反复出现的问题尤为重要，但一次性的不遵守情事如果是重大或蓄意的话，则同样值得关注。即使是很小的故障也可能表明当前流程和合规性管理系统存在严重缺陷。如果没有及时报告；它可能导致这样的观点，即故障并不重要，并且可能导致这种故障成为系统性问题。

合规报告应包括：

— 组织需要通知任何监管机构的任何事项；

— 合规义务的变化，其对组织的影响以及为履行新义务而建议采取的行动方针；

— 衡量合规绩效，包括不合规和持续改进；

— 可能的不合规的数量和细节，以及对它们的后续分析；

-采取的纠正措施；

— 有关合规管理系统的有效性，成就和趋势的信息；

— 与监管机构的联系以及关系的发展；

— 审计和监督活动的结果；

一，监控行动计划的完整执行，尤其是那些源自审计报告或监管机构要求或两者的行动计划。

遵守政策应促进对定期报告时间表以外出现的重要事项的立即报告。

A.9.1.5记录保存

记录保存应包括记录和分类合规性问题和所谓的不合规问题以及解决这些问题所采取的步骤。

记录应以确保其可读性，易于识别性和可检索性的方式存储。

这些记录应受到保护，以防止任何增加，删除，修改，未经授权的使用或隐藏。

组织的合规性管理系统记录可以包括：

— 有关合规绩效的信息，包括合规报告；

— 违规和纠正措施的详细信息；

一对合规管理系统进行审核和审计的结果以及所采取的措施。

A.9.2内部审核

审计职能，无论是内部审计还是外部审计，都应避免利益冲突，并且应独立发挥职能。

有关如何进行管理系统审核的信息，请参见ISO 19011。

A.9.3管理评审

管理评审还应包括以下方面的建议：

— 需要更改合规政策及其相关的目标，系统，结构和人员；

— 更改合规流程，以确保与运营实践和系统的有效整合；

— 未来可能发生违规情况要监控的区域；

— 有关违规的纠正措施；

— 当前合规体系和长期持续改进计划之间的差距或缺乏；

— 对组织内典型的合规行为的认可。

应将书面结果的副本和管理评审中的任何建议提供给理事机构。

A.10改进

A.10.1持续改进

遵从性管理系统的有效性的特征在于它具有不断改进和发展的能力。组织的内部和外部环境以及业务会随着时间而变化，客户的性质和适用的合规性义务也会随着时间的推移而变化。

合规管理系统的充分性和有效性应通过几种方法连续不断地进行评估，例如：审查或内部审核。

组织应制定措施以审查其合规性管理系统，并确保其保持最新并适合目标。在确定支持持续改进的行动的程度和时限时，组织应考虑其背景，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估控制的力度。持续改进的其他信息源可以是客户调查，引起关注的报告，定期监控，定期审核或管理评审的结果。

组织应考虑此类评估的结果和输出，以确定是否有必要或机会更改合规管理系统。

为了帮助确保保持合规性管理系统的完整性及其有效性，管理系统中各个元素的更改应考虑到依存关系以及此类更改对整个管理系统的有效性的影响。

在对合规管理系统进行更改时，组织应考虑这些更改对合规管理系统，其运营，资源的可用性，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不合格和纠正措施

未能预防或检测到一次性违规行为并不一定意味着遵从性管理系统通常无法有效地预防和检测到违规行为。

分析不符合项或不符合项的信息可用于考虑：

— 评估产品和服务绩效；

— 改善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；

— 重新评估是否需要通知有关方面；

— 提供潜在违规的预警；

— 重新设计或审查控件；

— 加强通知和上报步骤（内部和外部）；

— 传达有关违规的事实以及组织关于违规的立场。

组织应确定导致不当行为的根本原因，即不遵循政策或程序，或不遵循这两者，并根据吸取的经验教训更新政策和程序。