合规管理体系各要素之间的逻辑关系

雒宏伟（上海天祥质量技术服务有限公司）

在《中国认证认可》2018 年 7 期发表

摘要： ISO19600：2014《合规管理体系 指南》和相关国标的发布为企业建立或完善合规管理体系提供了指南。为了帮助企业更好的理解该标准，本文对标准中的“合规管理体系流程图”进行了解读，并在梳理标准的要求的基础上绘制了合规管理体系各要素之间逻辑关系图，最后对逻辑关系图进行了解释。

关键词：ISO19600 合规管理体系

Logical Relationships Between the Elements Of Compliance Management System

LUO HONGWEI Intertek China

Abstract: The issues of both ISO19600:2014 Compliance management system – Guidelines and correspondent national standard provide guidelines for companies to establish or improve their CMS. To help companies to understand better it this article explains the Flowchart of a compliance management system in the introduction of the standard and draws a chart of logical relationships between the elements of CMS based on analyzing the requirements of the standard and explains it at the end.

Keywords: ISO19600 Compliance Management System

ISO19600:2014及其对应的国标GB/T 35770-2017《合规管理体系 指南》的发布为企业建立和改进合规管理体系提供了指南。该国标将于2018年7月1日起实施。为了帮助企业更好地了解该标准，笔者基于本人最近几年对反贿赂和合规管理的研究成果和培训实践，将围绕标准理解和合规管理体系建设方面的一些重点问题推出一系列的有关ISO19600的文章。本篇将重点阐述合规管理体系各要素之间的逻辑关系。

在ISO19600:2014前言中给出了 “合规管理体系流程图”，如图1所示。

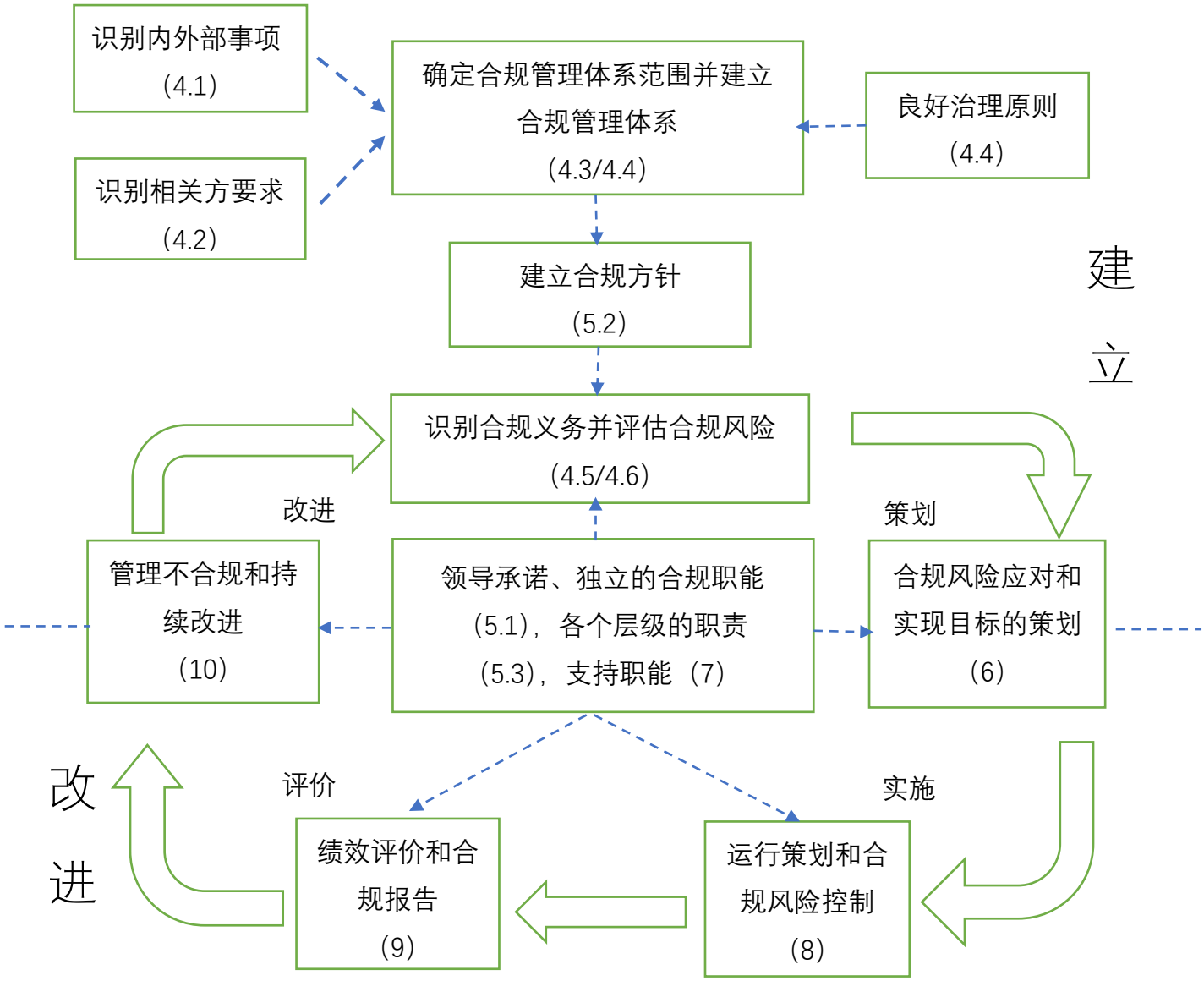

图 1:合规管理体系流程图

该流程图展示了合规管理体系的运作流程：

基于对组织与合规风险相关的内外部因素（4.1）的识别，以及合规管理体系的相关方及其要求（4.2）的识别，确定组织合规管理体系的范围（4.3），按照良好治理原则（4.4）建立、实施、保持和改进合规管理体系（4.4）。由治理机构和最高管理者为组织的合规管理体系确定合规方针（5.2），作为合规管理的基本政策指导合规管理的各项工作。识别与组织活动、产品和服务有关的合规义务（4.5），并对满足合规义务存在的合规风险进行识别、分析和评价（4.6），将组织的合规风险排列优先顺序。针对评价出来需要应对的合规风险制定控制措施（6.1）并建立合规目标以及目标达成的实施方案（6.2）。

组织策划满足合规义务的必要过程，并将确定的风险控制措施整合进入这些过程（包括外包过程）进行实施（8）。对合规义务的履行情况、合规风险控制的有效性等进行监视、测量、分析和评价（9.1），对合规管理体系进行内审（9.2）和管理评审（9.3），从而发现存在的不符合、不合规和改进机会。针对不符合和不合规分析原因制定纠正措施（10.1），对于改进机会，制定措施加以利用，确保体系的持续改进（10.2）。

整个体系是一个PDCA循环，其中4.5/4.6&6是策划（P）阶段，8是实施（D）阶段，9是检查（C）阶段，10是改进（A）阶段。体系的有效运作必须要治理机构和最高管理者的管理承诺（5.1）、确定组织各岗位的角色、职责和权限（5.3），并且需要一些支持性过程包括：提供必要的资源（7.1）、确保各岗位的人员具备应有的能力（7.2）、意识（7.3），通过组织全员和外部相关方的沟通和参与（7.4）以及确保各岗位得到最新有效的文件（7.5）。该流程图虽然展示出了主要过程之间的关系，但是比较简单，并没有全面的阐述合规管理体系各要素之间的逻辑关系。

为了帮助企业更好的理解ISO19600：2014标准要求，正确建立和有效运行合规管理体系，我们对合规管理体系各要素之间的逻辑关系进行分析，分析过程如下：

- 4.3"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 "。确定合规管理体系范围的考虑因素包括：组织环境、相关方要求和合规义务。
- 4.5.1 "合规义务的来源宜包括合规要求和合规承诺。" 4.2要求识别相关方的要求，这是合规义务的来源。
- 4.6 "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。" ；4.1 "组织宜确定其内部和外部问题，如与合规风险相关" 。这说明了合规风险和合规义务和组织环境的关系，合规风险是不能满足合规义务的风险，受组织环境的影响。虽然标准没有明确，但实际上合规风险的评价同样受到相关方要求的影响。
- 5.1 "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：确保确立组织的**合规方针**和合规目标" ；5.3.1 "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。" ；5.3.3 "治理机构和最高管理者宜任命或提名一个合规团队 :d)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 ;d)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 e)确保合规团队具备独立采取行动的权限。这是对组织良好治理原则的要求和体现。" 治理机构最高管理者宜确保合规方针目标的制定、职责的分配、管理体系的建立和良好治理原则的实施。

- 6.1 “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”， “组织宜策划应对合规风险的措施 “。4.1、4.2、4.4 和 4.5 是确定组织需要应对的合规风险的考虑因素，合规风险的应对措施主要针对的是已识别评价出的需要应对的合规风险。
- 6.2 “合规目标宜：a) 与合规方针一致；”
- 8.1“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”。运行过程的策划和实施要考虑组织的合规义务的落实和影响满足合规义务的合规风险的控制，这是运行控制的总则。
- 8.2 “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 “；“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。” 8.1 是总则，8.2 是要求落实识别出的合规义务和确定的风险控制措施，要求建立程序和文件化。
- 8.3 “组织宜确保外包过程受到控制和监视。”明确外包过程的控制，也是基于 8.1 确定的总则。
- 9.1.1“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“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”从中可以看出 9.1 的监视测量是针对合规管理体系及其主要过程和结果的监视测量。
- 9.2 “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”。审核是针对整个管理体系的符合性和有效性的评估。
- 9.3 “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” 。管理评审是针对整个合规管理体系。
- 10.1 对于监视测量、内审和管理评审发现的不符合、不合规和改进的机会制定纠正措施。
- 10.2“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。 “
- 整个第 7 部分是整个合规管理体系的支持性过程，包括 7.1 资源、7.2 能力和培训、7.3 意识、7.4 沟通和 7.5 文件化信息。

基于以上对 ISO19600:2014 标准要求的梳理分析，我们绘制了合规管理体系各要素之间的逻辑关系图，如图 2 所示。从该图我们可以看出：

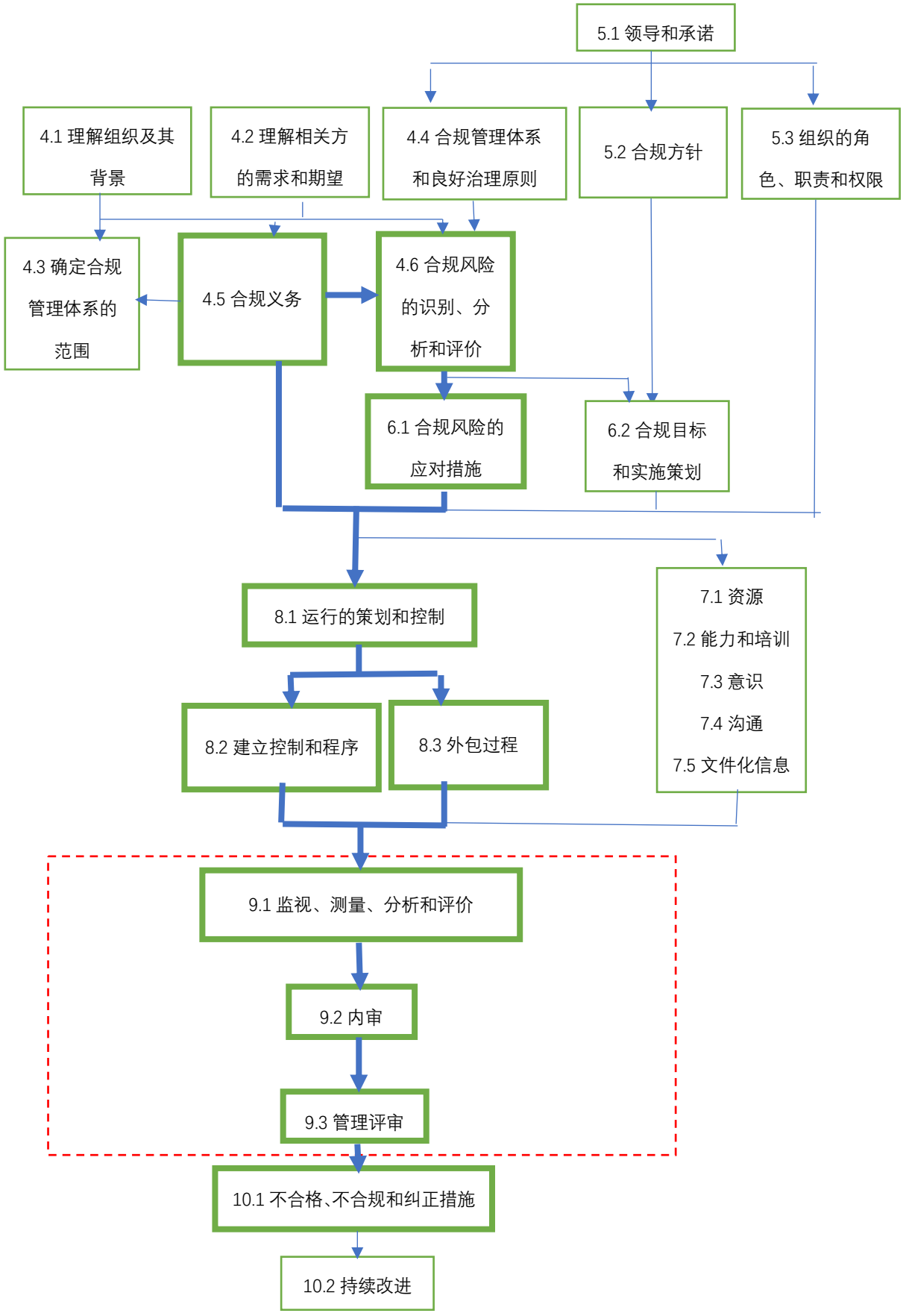

图 2 合规管理体系各要素之间的逻辑关系

1、合规义务（4.5）和合规风险（4.6）共同成为合规管理体系的的基础

整个合规管理体系是基于合规义务进行策划、实施、保持和改进的。识别组织的合规义务并满足合规义务是合规管理体系的目的，但是有些合规义务可以通过在组织的业务活动中进行直接落实，但是有些合规义务的履行存在一定的难度、利益影响、不确定性，也就是存在合规风险。因为不同合规风险的风险等级不同，有些会造成严重的后果如：质量事故、环境事故、安全事故，贿赂案件、受到处罚等，需要有针对性的制定一些控制措施。因为合规风险可能很多，组织资源是有限的，为了提高合规管理体系的有效性，这就需要进行风险的评价，对风险排列优先顺序，并作为合规管理体系策划的基础。因此我们在策划合规管理体系时， 既要考虑识别出的合规义务（4.5），也要考虑对应合规义务存在的合规风险（4.6），将其共同做为合规管理体系的核心和基础。

2、合规管理体系的一条主线和 PDCA 循环

合规管理体系的建立，首先要识别合规义务（4.5），针对合规义务进行合规风险识别评价（4.6），针对评价出来的较高合规风险，制定相应的控制措施（6.1）。这些措施和合规义务要融入组织的业务过程，或者作为业务过程的控制准则（8.1），针对合规义务和相应的合规风险建立相应的控制和程序（8.2），对于外包服务过程，基于其对组织带来的风险和风险程度对外包过程进行控制（8.3）。对控制措施的有效性和合规管理体系的绩效进行监视测量（9.1），对合规管理体系进行内审（9.2）和管理评审（9.3）。针对发现的不符合和发生的不合规制定措施并进行实施（10.1）。图 2 加粗的部分从 4.5----10.1 这是合规管理体系的一条主线，起始于合规义务和合规风险，将合规义务和风险控制措施融入组织的业务过程，并通过合规义务落实情况和合规风险控制措施有效性的监视测量改进，最终确保达到控制风险满足合规义务的目的。这条主线也是一个 PDCA 的循环，其中 4.5、4.6 和 6.1 是策划（P）阶段，8.1，8.2 和 8.3 是实施阶段（D），9.1、9.2 和 9.3 是检查（C）阶段，10.1 是改进（A）阶段。

3、合规管理体系的三级监控

图 2 中虚框中 9.1 监视测量是针对合规管理体系的日常的监视和测量，9.2 内审是对整个管理体系的定期评价，9.3 管理评审是由最高管理者基于管理体系各方面的信息对管理体系的适用性、充分性和有效性的评价，这是合规管理体系的三级监控，共同监控合规管理体系对于控制合规风险和履行合规义务的有效性。

4、领导和承诺

领导承诺主要体现在确立合规方针（5.2）和合规目标（6.2）、建立和改进合规管理体系并落实良好治理原则（4.4）、分配职责和权限（5.3）等。

参考文献

【1】 ISO， ISO19600:2014 Compliance management system – Guidelines

【2】 SAC， GB/T 35770-2017 《合规管理体系 指南》

作者简介

雒宏伟，工商管理博士。研究方向：反贿赂管理、合规管理、资产管理、道路交通安全管理 。INTERTEK 集团上海天祥质量技术服务有限公司 ISO37001、ISO19600、ISO39001 和 ISO55001 项目经理。