浅析合规管理体系的基本原则

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：合规已经成为当今企业面临的最大挑战，企业迫切需要通过建立有效的合规管理体系来防范合规风险。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，本文对标准进行了分析的基础上，归纳整理出了 “合规管理的七个基本原则”，并对每个原则结合标准要求进行了说明。

关键词：ISO19600 合规管理体系

Simple Analysis of Principles of Compliance Management System

LUO HONGWEI Intertek China

Abstract: Compliance has become the largest challenge facing companies, so it is essential for companies to establish compliance management system to prevent compliance risks. 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 summarizes out seven principles of compliance management based on analysis of the standard and gives every principle an explanation combining with requirements of ISO19600.

Keywords: ISO19600 Compliance Management System

合规已经成为当今企业面临的最大挑战。现在基本上每周都会有新的法律法规的出台，没有有效合规控制、没有良好的合规文化可能意味着数以百万美元的罚款、甚至更多。“中兴通讯事件”更是给企业敲响了警钟，企业迫切需要通过建立有效的合规管理体系，来防范合规风险。

由 ISO 项目委员会 PC271 制定的 ISO19600：2014《合规管理体系 指南》给想实施合规管理体系或者希望为其合规管理寻找标杆的企业提供了全面的指南。2017 年 12 月 29 日，GB/T 35770-2017《合规管理体系 指南》国家标准经国家质量监督检验检疫总局、国家标准化管理委员会正式批准、发布，并将于 2018 年 7 月 1 日起实施。GB/T 35770-2017 是基于 ISO19600:2014 的等同转换发布的国家标准，该标准的发布将有力推动 ISO19600：2014 在国内企业的实施、帮助企业提升合规管理水平。

ISO19600：2014《合规管理体系 指南》同样采用 ISO 针对管理体系提出的统一的高级结构：统一的管理体系框架、统一的通用部分的管理体系要求和术语。虽然这些管理体系标准看起来非常相似，但是每个管理体系标准都有其独特的基本原则，比如质量管理体系的七项质量管理基本原则。只有正确理解这些基本原则才能够正确理解标准要求。为了帮助企业更好的理解 ISO19600：2014《合规管理体系 指南》，我们对 ISO19600：2014《合规管理体系 指南》进行了分析。虽然标准第一部分范围中明确提出了 “良好治理、比例原则 、透明性和可持续性原则”，但是并没有进行解释和说明，另外结合笔者对该标准的研究，我认为合规管理体系还有些其它的基本原则，并将其归纳整理成为 “合规管理的七个基本原则”。

一、良好治理结构(good governance)

在其它管理体系通常的组织架构的基础上，在 “最高管理者” 上面增加了 “治理机构”， 目的在于：强调最高管理者领导作用和承诺的同时，增加了对最高管理者的监督。另外突出了合规团队的角色、职责和独立性，如指南4.4 “考虑如下治理原则：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。” 同时指南5.3明确了治理机构、最高管理者、合规团队（compliance function）和管理人员（management）和员工在合规管理方面的职责。该指南在强调合规团队的重要角色和职责的同时，强调包括各级管理人和员工的全员参与。这样的治理架构是保证合规管理体系能够有效运作的基本保障。

二、以合规义务(compliance obligation)为中心

合规管理体系的最根本的目的是识别和满足组织的合规义务，避免不合规给组织带来的经济和声誉以及其他损失。整个体系围绕着合规义务的，如：4.5**合规义务**整个条款是对合规义务识别和更新的要求；4.6要求 “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” 、 “**合规义务改变**时重新进行合规风险评价” ；5.1要求 “治理机构和最高管理者宜确保**运行指标和合规义务保持一致**” ；5.2.1要求 “方**针宜适合**于组织活动产生的**合规义务**” ；5.3.2要求 “治理机构和最高管理者的积极参与和监督确保**员工有效地履行合规义务**” ；5.3.4要求 “合规团队宜与管理者合作负责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” ；5.3.5要求 “管理人员宜负责提高员工**合规义务的意识**、**将合规义务纳**

入他们职责范围内的现有业务实践和程序、对外包业务进行监督，确保**合规义务被纳入**考量”；5.3.6要求“包括管理者在内的所有员工宜坚持**履行**与其职位和职务有关的**组织合规义务**”；6.1要求“组织进行合规管理体系策划宜**考虑4.5识别的合规义务**”；7.2.2要求“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**”、“**合规义务**尤其是法律或相关方要求**改变时**宜考虑再进行合规培训”；7.3.2.3要求“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**”；8.1要求“组织宜计划、实施和控制**满足合规义务必需的过程**”；8.2要求“宜有控制措施**管理识别的合规义务**和相关合规风险并实现期望的行为”、“宜建立、文件化、实施和保持程序支持合规方针并**实践合规义务**”、“制定这些程序宜考虑**将合规义务整合到程序中**”；8.3要求“组织的运行**外包通常不减轻**组织的法律职责或**合规义务**”；9.1.2要求“典型的合规管理体系监视包括**有效分配满足合规义务的职责、合规义务的宣贯程度**”、“典型的合规绩效监视包括**未履行合规义务的案例**”；9.1.8要求“合规报告包括**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”；10.1.2要求“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”。

三、合规管理投入应与合规风险相称(proportionality)

因为法律法规很多，组织需要承担合规义务也会很多，组织资源不可能是无限的，而且组织也不可能把所有资源用于合规管理，因此为了提高合规管理体系的绩效和有效性，需要对影响履行合规义务的**合规风险**进行识别、分析和评价（4.6），从而对其排列优先顺序，为资源分配和合规管理体系的设计和改进提供依据。合规管理应与合规风险相称，风险越高合规管理的投入越大，反之风险越低合规管理的投入越小甚至是维持原有措施。

合规管理体系的一些条款围绕合规风险提出了如下要求：4.1“组织宜确定其与**合规风险**相关内部和外部问题”；4.4“合规管理体系宜反映组织的价值观、目标、战略和**合规风险**”；5.2.2“制定合规方针，宜考虑与**不合规有关的风险性质和等级**”；6.1“组织进行合规管理体系策划，宜考虑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”；7.2.2“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**”；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（**合规风险**的应对措施）确定的措施”；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**”；8.3“组织宜考虑与过程有关的**第三方相关的合规风险**”；9.1.6指标制定过程“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**”。

但是正如指南所说“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。

四、将合规管理体系要求与组织业务过程整合(integration)

指南在一些条款将合规与组织业务活动进行整合进行了明确要求，如：5.1 “治理机构和最高管理者**确保合规管理体系要求融入组织的业务过程**”；5.2.1 “合规方针宜**明确合规融入运行的方针、程序、过程的程度**”；5.3.4 “合规团队宜与管理者合作，负责**将合规义务融入现有的方针、程序和过程**”；5.3.5 “管理人员宜负责其职责范围内的合规，**将合规绩效纳入员工绩效考核，将合规义务纳入他们职责范围内的现有业务实践和程序**；” 6.1 “a)**将措施整合进入合规管理体系过程并实施**”；8.1 “组织宜计划、实施和控制满足合规义务必需的过程，并**通过确立过程准则实施6.1确定的措施**”；8.2 “制定合规程序宜考虑将**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”；9.3 “合规过程的改变以确保**与运行实践和体系有效整合**”。从指南这些要求可以看出，合规管理体系不是要求组织另外建立制度或文件，而是要求合规要融入运行的方针、程序、过程，将合规管理体系要求作为组织业务过程控制的准则，同时将合规绩效纳入员工绩效考核。

五、建立合规文化(compliance culture)

指南的引言中强调了建立合规文化的重要性，指出 “通过将合规植入组织的文化以及为其工作的人的行为和态度中实现可持续合规”，并提出建立合规文化的方法-- “组织实现合规的方法最好是由领导采用核心价值和普遍接受的公司治理、道德和社会标准来打造。将合规植入为组织工作的人的行为中依靠各层级领导和组织的清晰价值观以及对推动合规行为措施的认知和实施。如果组织各层级做不到这样，就有不合规的风险。” 在指南的一些条款中也对建立合规文化提出了如下要求：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：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**的方式”；5.2 “确立的**合规方针宜与组织的价值观、目标和战略保持一致**”；7.2.2 “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**”；7.3.2.2 “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**；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**”；7.3.2.3**合规文化**明确了发展合规文化对治理机构、最高管理者和管理层的要求，并列举了合规文化的形成体现；9.1.2 “典型的合规绩效监视包括**合规文化的情况**”；9.1.7 “组织鼓励和支持**充分和坦诚报告的文化**”。

六、增强合规信息的透明性（transparency）

增强合规信息的透明性、及时报告合规信息是震慑、发现和应对不合规或不符合的有效手段。通过举报违规行为、报告合规信息，使得不合规或不符合引起重视并采取措施进

行控制或处理，从而降低合规风险。指南中对合规信息的报告提出了如下要求：5.1 “治理机构和最高管理者**确立并维护问责机制**，包括**对合规事件和不合规及时报告**” ；5.2.1 “合规**方针宜明确管理和报告合规事项的责任**” ；5.3.1 “治理机构和最高管理者宜**为合规团队分配职责和权限**以向治理机构和最高管理者**报告合规管理体系的绩效**” ；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确保建立高效及时的报告系统**” ；5.3.6 “包括管理者在内的所有员工宜**报告合规疑虑、问题和失败**” ；7.3.2.2 “最高管理者的关键职责包括**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**” ；7.4.3 “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**” ；8.2 “制定合规程序宜考虑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；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**”;9.1.1 “组织宜**确定何时应**分析、评价和**报告监视和测量的结果**” ；9.1.7**合规报告制度**和9.1.8**合规报告的内容以及**10.1.2**上报**三个条款是专门针对报告合规信息的；9.2 “组织**宜确保审核结果报告给相关管理层**” 。10.2 “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**” 。

七、合规管理的可持续性（sustainability）

合规是组织可持续发展的基石。指南的引言中指出 “合规管理体系与其它管理体系一致，**以持续改进原则为基础制定**的” 、 “通过将合规植入组织的文化以及为其工作的人的行为和态度中实现**可持续合规**” ，而且引言中的合规管理体系流程图清晰描绘了合规管理体系是按照PDCA循环达到持续改进的目的。当然，指南的一些条款也对持续改进提出了明确要求，如：4.4 “组织宜确立、制定、实施、评价、维护和**持续改进合规管理体系**” ；4.5 “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**” ；5.1 “治理机构和最高管理者宜**推进持续改进**” ；5.2.1 “合规方针包括**持续改进合规管理体系的承诺**” ；5.3.4 “合规团队宜与管理者合作负责**为员工提供或组织持续培训**” ；6.1 “组织**进行合规管理体系策划实现持续改进**” ；7.1 “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**” ；7.2.2 “**对员工的教育和培训**宜在组织成立时就提供并**持续提供**” ；7.3.2.2 “最高管理者的关键职责鼓励员工**提有利于合规绩效持续改进的建议**” ；7.4.2 “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**” ；8.2 “宜维护、定期评价并试验这些控制，以**确保控制的持续有效**” ；9.1.2 “宜制定**持续监视计划**” ；9.1.3 “**反馈宜是持续改进合规管理体系的重要来源**” ；9.1.7 “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**；9.1.8 “**合规报告包括**对合规绩效的测量，包括不合规和**持续改进**” ；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**” 、 “管理评审宜考虑**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 “；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**。”。

从以上分析可以看出，合规管理的这七项基本原则充分体现在 ISO19600:2014《合规管理体系 指南》的各条款的要求中，其中 “良好的治理结构” 是合规管理体系有效运作的保障，而整个合规管理体系 “以合规义务为中心”，通过识别合规义务并识别分析评价满足合规义务存在的合规风险，针对识别出的合规风险制定措施、根据风险的大小投入合规管理资源，使 “合规管理投入与合规风险相称”，将风险控制措施和 “合规管理体系要求与组织的业务过程整合” 以提高合规管理措施的有效性，通过 “增强合规信息的透明性” 以达到及时发现违规行为和不符合、进行纠正并制定纠正措施， 最终实现满足合规义务的目的，并通过 “建立合规文化” 和持续改进的机制确保合规管理的 “可持续性”。

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。