

白皮书

# **游戏规则已经改变：**

**真正高效的合规项目的十大基本要素**

## 执行概要

各行各业的很多公司由于法律和法规合规性问题而遭受到了严重的声誉和经济损失，对此我们屡见不鲜。其中，大多数公司都认为自身具备合理的合规流程，但不知何故，这种流程并未发挥作用。公司将越来越多的企业资源用于满足合规性，同时更加关注高层和董事会，但担忧仍然挥之不去，而这显然事出有因。除了密切关注监管行动之外，法律和合规高管还力图将合规计划从不相干的要素变为一个完整的整体。但是现在，我们看到主要监管机构的目标以及他们在决定是否采取执法行动时所考虑的因素都已发生了重大转变。鉴于这一背景，同时考虑到真正在“现实世界”中起作用的近期经验，组织在开发高效的合规计划时思路更为清晰。本白皮书概述了这些规则改变者，提供了包含 10 个必需要素的路线图，在管理层和董事会实现合规目标所需的计划中，这些要素可谓不可或缺。

## 引言

如果您是 CEO、总监、总顾问、合规官、风险官，或者是贵组织法律和法规合规性方面的负责人，即便不提心吊胆，也总会感觉惴惴不安。您会考虑与供应商、产品责任、营销、反垄断、并购和联盟伙伴（包括转售商、分销商、代理和合资伙伴）相关的风险……似乎需要担心的风险无穷无尽。您也感觉贵组织的人员了解不当行为，但并未采取行动。您在合规计划上投入了很多的时间和精力，并尽力尝试衡量结果，但并不确定这种计划真正有效。

近些年来，各个行业都出现了因合规性方面的执法行动而被击溃的企业。的确，法律和法规合规性问题已成为高层和董事会关注的焦点，为战略、运营执行、风险管理和管理层薪酬制度带来了挑战，从而引起了人们的广泛关注。“业务运行”占用了绝大多数的时间，尽管合规成本持续增加，但很多企业的合规计划仍有许多有待改进之处。

管理层和董事会常常听到证监会和司法部官员谈及“萝卜加大棒”的方法，即：执法时对强大的合规计划给予更多的宽容，而对较弱的计划则施加更严格的控制。董事们了解特拉华州大法官法庭和最高法院案例，因此强调董事会有责任确保合规计划的有效性。此外，人们还关注更新后的联邦量刑指南，该指南旨在处理犯罪行为以及用于评估和降低相关风险的公司计划。

新法规对金融服务造成了巨大冲击，仅在去年，就发布了超过 2,000 页的新规定，席卷六大法律领域。人们预计，一段时间以后，仅 Dodd-Frank 法规就将达到 5,000 页。金融业努力塑造即将出台的规定，以确保未来的业务前景和行业健康发展，不过这已变得越来越困难。<sup>i</sup> 但毫无疑问，法律和法规合规性方便的问题涉及到所有行业，因此要想保持合规将会愈加困难。

## 新的监管方向

多年来，SEC 和 DOJ 一直强调他们在调查和执法行动中如何为公司提供“信用”，以便让其获得有效的合规计划。很多总顾问、首席合规官等以此为战略核心，作为强化内部计划的诸多理由之一。但直到最近，几乎没有直接证据表明监管机构的消息具有行动支持。的确，人们关注得更多的似乎是在故障发生之后开发有效的合规计划，而不是在事实发生之前授予信用。此外，企业也发现与执行相关的监管模式参差不齐，因此他们需要清晰性和一致性。而现在，规则改变者出现了，这一点非常值得密切关注。

<sup>i</sup> 如欲了解有关金融服务业的更多信息，敬请查看 IBM 在 2012 年发布的白皮书《合规之路上的坑洞 - 企业法规合规性计划的六个常见陷阱 (Potholes on the Road to Compliance – Six Common Pitfalls of Enterprise Regulatory Compliance Initiatives)》。

该案例涉及的是 Morgan Stanley。据报道，合规问题出现的缘由是一位名为 Garth Peterson 的总经理成功帮助该公司向一家中国国有企业销售了不动产，但结果证明，这是一家由 Peterson 直接控制的空壳公司，相关现金已经全部支付给了中国官员及其本人。Peterson 承认有罪，可能面临六位数的罚金和五年监禁。然而，Morgan Stanley 发生了什么，或者说没有发生什么，才是我们这里真正要探讨的内容。DOJ 和 SEC 决定不针对该公司采取任何执法行动。究其原因，在于 Morgan Stanley 已经拥有强大的合规系统，包括相关的内部控制措施。该公司会定期更新控制措施，以应对不当行为风险，为员工提供大量培训、合规提示、年度员工确认和持续监控。当出现不当行为的证据时，该公司会立即启动并实施彻底的调查。

除了具有强大的合规流程之外，最后一点也与决定不追究此事的监管机构直接相关 - 该公司及时上报并彻底调查了此事。作为对比，我们可以看看最近 Wal-Mart 所经历的惨败。相信您已经听说了事情的来由：Wal-Mart 的高管知悉公司将向墨西哥政府官员支付数百万美元，希望这些官员帮助该公司在墨西哥进行扩张，但却停止了针对该项目进行的调查。DOJ 和 SEC 对此高度关注，公司恐怕难逃一劫。监管机构最介意的一点在于高管未报告可疑或已知的违规，并且未能进行完整而全面的内部调查 - 而在调查开始后将其终止只会让问题变得更加复杂。而现在，有相关迹象显示这次贿赂事件可能不仅限于墨西哥子公司。Wal-Mart 的股票价格因此遭受了重创，该公司还可能面临巨额罚金，高管可能被判入狱，而投资者也在起诉。

在前面的示例中，我们看到了两家知名品牌企业，一家很可能需要付出沉重的代价，而另一家则毫发无损。事实上，由于清晰地展示了有效合规和操作系统，Morgan Stanley 甚至还因此提高了自身声誉。两个公司的做法大相径庭，因此结论不言自明。一个是急于掩饰，因此不得不应付强大的监管机构和愤怒的股东；而另一个则建立了高效的合规系统，有所为有所不为，因此监管机构以及其他各方会善意地加以对待。

## 何谓“高效”？

有关哪些因素构成高效的合规流程以及如何开发和维持该流程，合规官员看到了大量信息。监管机构在司法部门的一系列备忘录中提出了指导，包括 McNulty Memo，其概述了高效系统的五大“必备要素”。此外，联邦量刑指南也提供了方向。<sup>ii</sup>

诚然，严格按照监管机构的条款来保持合规流程不失为一个好主意，但拥有真正高效的流程更为重要。也就是说，制定了合规计划，且此类计划有助于成功避免重大不合规事件的企业，通常会远离监管机构的视野。而通过避免监管调查和执法行动，将能产生诸多业务效益。

那么，假设监管机构的要求真正与确实有效的措施相一致呢？那就将成为一个绝佳的模型。而我们现在看到，有一个监管机构似乎已经找到了正确的答案 - 建立在之前的监管指导之上，着眼于“现实世界”中真正有效的因素 - 这就是 SEC 的监管和审查合规官。

---

<sup>ii</sup> 我认为一个特别有用的来源是 IBM OpenPages 发布的 2010 年白皮书《不合规的昂贵代价 - 从高效的合规计划收获回报 (The High Cost of Non - Compliance - Reaping the Rewards of an Effective Compliance Program)》。(撰写本文之时，无可否认我的观点有失偏颇，尽管本文在合规社区中广受欢迎。)

## SEC 的 OCIE

如果您处于金融服务业，就知道 OCIE 的关注点非常广泛，包括促进合规、防止欺诈和监控风险。<sup>iii</sup> 就欺诈而言，审查人员会识别欺诈行为指标，如内幕交易、市场操纵和庞氏骗局，并与 SEC 的执法部门合作追击这些事件。对组织进行审查时，OCIE 会广泛撒网，不仅涵盖证券经销商、过户代理人、投资顾问和投资公司（根据 Dodd-Frank 法规，现在还包括私人股本和对冲基金），还包括证券交易所、清算机构、信用评级机构、金融业监管局、公众会计公司监督委员会等。但重要的是，其理事 Carlo di Florio 以超越行业的方式概述了构成高效合规计划的要素。

Di Florio 直接向 SEC 主席 Mary Shapiro 报告，他带领着一支由 900 人组成的专家团队，负责在 11 个区域性办事处及其位于华盛顿的总部开展工作，推进 OCIE 流程，提供有关如何实施审查的洞察力。通常，OCIE 人员首先查看公司的组织、工作流程和控制环境。随后，他们审查相关文档，与包括第三方在内的一系列公司人员进行面谈，重点关注政策和相关程序，包括政策管理以及处理不断演变的条件时的灵活性。他们着眼于沟通和培训的有效性，同时关注公司的责任分配和处理方式。此外，监测和测试流程、上报问题的规程以及内部举报流程也在他们的考察范围之内。

近期，OCIE 将关注点扩大到了一些关键问题上，如由谁掌握组织权力（事务性部门还是法律和合规部门）、奖金池如何分配、合规人员的独立性及其参与关键决策的情况。此外，他们还考虑了业务部门的合规性对于绩效评估和奖励流程的影响程度。

Di Florio 表示，现在审查范围延伸到了高管和其他员工之外，涵盖了对公司董事会成员的直接面谈。这成为了认识公司合规文化的关键环节，通过与董事面谈，可以了解董事会和高层管理人员对于法规合规性问题的重视度和关注度。Di Florio 并未公开提及公司名称，但据媒体报道，这种讨论已经在 Goldman、Morgan Stanley、Barclays 和 Wells Fargo 之类的企业中展开。据他表示，之所以出现这种新的焦点，部分原因在于公司的合规文化“概念晦涩难解，极富挑战性”，对公司的道德行为具有巨大的影响，同时也注意到了将合规性并入风险治理流程的必要性。

为了总结构成高效合规流程的要素，di Florio 指明了相互配合的十大要素（见下一页的侧边栏），同时，这也反映了美国联邦量刑指南。

Di Florio 为我们展现了对于他和他的团队如何执行 OCIE 的广泛任务的重要洞察力。曾与 di Florio 共事的人都知道，他的方法深思熟虑且极富创造性；尽管他言行举止温文尔雅，但却在坚持不懈地追求 OCIE 的目标。但这里的关键提示在于，他在审查中所关注的正是经验表示确实有效的要素。

---

<sup>iii</sup> 有关 OCIE 方法的更多信息，请参阅 di Florio 的相关陈述，如 2011 年 10 月 17 日发表的“合规和道德在风险管理中的角色 (The Role of Compliance and Ethics in Risk Management)”，另见相关媒体报道，如 Accelus 于 2012 年 4 月 4 日在 Thomson Reuters 上发表的报道“SEC 审查者进入美国董事会测量合规性 (SEC Examiners Enter U.S. Boardrooms to Gauge Compliance)”。本文中的部分材料来自最近几个月以及过去一年中我与 Carlo di Florio 的通信，摘自 2012 年 6 月的《合规周刊》专栏。

## 让合规流程高效的要素

让我们深入了解一下每一个要素，因为对这些要素加以整合，便能打造出真正高效的合规计划。我们在此建立这个大纲的目的是总结多年的经验，在此过程中，合规计划已从存在多方面不足的初级阶段演变成为一种全局式方法，进而形成了一个路线图，有助于我们打造在企业世界真正高效的计划。

**治理。** 尽管部门所谓的专家对此慷慨激昂地提出异议，但董事会并不直接负责合规性 - 这是管理人员的工作。这么说来，董事会的确肩负着监督合规计划的重要职责，但他们应该可以完全信任管理人员，相信他们已经建立了高效的流程。为了达到这个目的，董事会必须从 CEO、首席合规官等人员处接收定期发送的报告，了解有关流程设计和运作以及反映流程有效性的信息（更多相关信息，请参阅下文“指标”中的内容）。然而，我们看到有些公司设计合规计划的主要目的是为董事会开发报告，坦率地说，这些计划的效果并不好。报告应该是有效合规管理的自然衍生物，优先考虑事项应是确保推动有效合规的心态和行为。

**文化、价值观、责任。** 对于实现高效合规而言，最重要的也许莫过于组织文化，包括建立在道德价值观和明确问责制基础上的高层态度。企业文化最重要的基础是最高管理层的行为，该行为必须与其言辞一致，并获得整个组织范围内的管理人员和监督人员的支持。如果缺乏完整性，合规计划就只能流于外表而缺乏实质内容，随着时间的推移，这种计划必然无法达成其设计目的。毫无疑问，具备完整性和道德价值观的组织能够吸引最优秀的员工、客户、供应商和合资伙伴等。尽管很难直接将积极文化与企业成功关联起来，但有的指标却表明了这种关系。Edelman Trust 在其 2011 年的 Barometer 中发现，85% 的全球受访者表示从自己信任的公司购买产品或服务，而 73% 的受访者表示拒绝从自己不信任的公司购买产品或服务。<sup>iv</sup> 此外，另一家组织 Ethisphere Institute 也看到了这种关联性；其发现，长期而言，具有高度道德的公司比竞争者的绩效每年高出 7% 到 8%。<sup>v</sup> 确实，当组织中存在为人们所共享的良好价值观时，员工更倾向于在各个方面做正确之事，包括但不限于坚持适用法律和法规的字面含义和内在精神。此外，这些组织具有相关流程，可以确保个人在进行业务决策时为自身的行为负责。

**治理：**董事会和高层管理人员在顶部设定一个基调，为合规和道德计划提供必要的资源、独立性、地位和权威。

**文化和价值观：**领导层促进整个组织范围内决策制定的完整性和道德价值观，建立问责制。

**激励和奖励：**将完整性和道德价值观纳入绩效管理系统和薪酬体系，鼓励和奖励正确的行为，坚决处理不当的行为。

**风险管理：**确保采取有效的流程识别、评估、缓解和管理整个组织范围内的合规和道德风险。

**政策和程序：**根据业务、风险、法规要求和利益冲突建立、维护和更新政策和程序。

**沟通和培训：**根据具体业务、风险、法规要求进行基于角色的培训，让合规流程中的每个人都能了解自身角色和职责。

**监视和报告：**监视、测试和监督功能评估系统的健康性，向管理层和董事会报告关键问题。

**上报、调查和管制：**确保存在员工能够秘密地匿名提出问题的流程，无须担心遭受报复，同时根据公平一致的规章制度调查和解决提出的问题。

**问题管理：**确保对已确定问题开展根本原因分析，以便及时采取有效的补救措施。

**持续改进：**确保组织积极与开发成果和领先实践保持同步，将其作为持续改进文化承诺的一部分。

<sup>iv</sup> 2012 年 6 月 8 日《合规周刊》

<sup>v</sup> CSR Wire.《遵守道德是值得的：与 Corpedia 创始人 Alex Brigham 的对话 (It Pays to be Ethical: A Conversation with Corpedia Founder Alex Brigham)》.2012 年 5 月 30 日

**激励和奖励。**与责任紧密相连的是针对道德行为设置有意义的激励策略以及相关的奖励和纠正措施。我们看到，很多公司高管尽管说得天花乱坠，但却未能将合规性嵌入人力资源流程中。合规职责必须纳入目标设定和绩效评估以及相关的晋升和薪酬调整流程中。同样，合规性并非完全是合规官员的职责，而在于各个责任领域的每一位一线管理人员和人事经理。该方法是将合规性嵌入到业务流程中的各个必需部分，这不仅能提高合规的有效性，还可让合规流程更为高效。如果合规在现有程序之上叠加，那么管理成本就将飙升。如果将其嵌入到管理流程之中，便可避免不必要的额外成本，同时，正常的管理流程也能让它发挥良好的作用。

**风险管理。**业务流程必须反映相关的合规相关风险，同时在业务流程中建立政策和协议，以管理潜在的风险暴露。风险鉴定内容包括不合规可能发生的位置和方式、发生的可能性、发生时将对公司产生的影响、风险事件可能产生这种影响的速度。识别风险和需求后，便可根据需要放置资源，让其发挥最大的作用，从而将风险降低至可以接受的水平。

**政策和程序。**政策管理本身已经成为了一门艺术，而这并非毫无来由，因为书面政策构成了适当动作和行为的基础。我们曾看到用法律术语编写的政策，这些政策具有不同的要素和格式，处于不同的完成或更新阶段，在需要时很难使用。同样，员工很难或几乎无法知道哪些行为在日常情况下可接受或不可接受。政策应该具有标准化格式，且应基于风险、目的明确、表达清晰、易于理解和使用，同时还应为员工所信任，让他们知道该政策已获得批准且可以信赖。应对政策的生命周期进行管理，根据最新的法律法规建立资料库，跟踪、审查和批准版本控制和更改，同时链接到具体的业务活动和修改后的责任 - 任何异常处理都应进行适当的批准和记录。同样，政策应依靠并链接至嵌入业务流程的良好程序。公司最不想看到的事情，莫过于发现自身具备书面政策，但不为相关行动所支持。

**沟通和培训。**组织中的每个人都必须了解组织对其所担任角色的期望，特别是要了解为什么满足这些期望非常符合自身和组织的最佳利益。员工必须了解规则背后的原因 - 为了帮助公司及其员工、客户以及其他的人。事实上，如果员工不了解某项措施背后的原因，就会以完成清单的心态走过场，甚至将规则忽略不计。在组织中，必须从上至下进行充分的沟通，证明高层管理人员对合规计划的支持。同时，培训项目也应落实到位，不仅限于录用之时，还应进行持续的培训，以教室和计算机为媒介，辅之以部门负责人提供的在职强化。有关潜在不合规问题的信息必须通过常规管理路径或单独的通道进行沟通，以便采取适当的行动和跟进措施。信息不仅应在组织内纵向流动，还应进行横向流动，改变孤岛思维，让整个公司范围内的各级管理人员都能根据需要自由沟通。我们知道，若要鼓励和促使人们及时上报潜在的不当行为，开放、可访问、有效的内部或外包举报渠道非常重要，同时还必须采取措施确保该渠道获得充分信任。此外，还可从社交媒体站点和离职面谈以及内部审计结果中获得相关信息。

**监视和报告。**这些要素非常重要，应该将其融入到业务和管理流程的核心。当最接近行为的监督管理人员知悉活动并在正常的业务管理过程中对其进行监视时，合规最为有效。向上报告极其重要，但如上所述，它不应成为基本合规流程设计的基础。事实上，报告应与管理流程中的信息流整合，由合规办公室负责进行监视，确保就相关信息进行及时、有效的沟通。同样，流程和信息流测试也可由一线管理人员在正常的业务部门运转过程中完成，同时由内部审计职能部门协同合规办公室和业务部门领导执行其他有针对性的测试。

**上报、调查和管制。**员工必须能够自由提出问题，并认识到秘密提出问题的重要性，必要时可以采用匿名的方式。在具有正确的文化和道德价值观的组织中，员工通常能够自由地通过正常报告渠道上报潜在的不当行为，并且上报后将产生效果。与此同时，存在替代渠道也非常重要，如热线电话或举报渠道，这种渠道应值得信赖，可以根据需要使用。这种信赖的基本特征在于坚信不会遭受报复，并且相信报告人员将获得称赞。经验表明，决定成败的因素在于员工最终是否因其报告而收到了采取行动的通知。如果人们认为自己的报告不会被认真对待，流程中缺乏适当的惩戒性措施，那么这种流程注定会失败。

**问题管理。**当出现合规问题时，必须采取行动，以便了解发生了什么、事件的严重程度和影响，以及必须采取哪些补救措施。内部报告应在管理层中逐级向上展开，如果应当上报董事会，那么还应适当地考虑进行外部报告。应对事件展开分析、分类和分配，以便后期跟进。如果情况足够严重，则应考虑展开调查，还可根据需要聘请外部法律或其他顾问。处理手头上的问题固然重要，但同样还需要了解合规流程为何未能阻止事件发生、重新评估相关风险、确定可能需要采取哪些系统性纠正措施，如改进流程、规程、控制措施或合规流程的其他方面。

**持续的改进流程。**与业务流程中的其他要素一样，环境和实际情况一直在演变，因此，管理人员应始终与新发展保持同步。新的法律法规和相关的法律案例不断出现，技术进步层出不穷，经验也在逐渐变得丰富，这些都在不断塑造着领先的实践。经验表明，效果最好的方法是由法律顾问负责跟踪新的规定和要求，然后就其影响通知相关业务部门和合规办公室。法律和合规办公室协同业务部门确定需要对广泛适用的政策做出哪些改进。通常，业务部门本身最有资格确定应该对业务流程中的程序和协议做出哪些更改，而合规办公室通常负责监督。



## 更多注意事项

除此之外，还有几个额外的因素对于达成真正行之有效的合规计划而言至关重要。

**指标。**长期以来，合规职能部门一直力图衡量企业合规计划的有效性 - 这种目标或许是一种展示和提高绩效的自我欲望，或者是 CEO、董事会、监管机构或业务合作伙伴的要求。多年来，很多人看到的衡量指标是不合规事件的数量和类型、公司热线电话的呼叫次数或举报渠道的使用次数。随着时间的推移，人们已经明显发现，这种指标无法充分解决固有的风险，或影响公司员工的思维模式。不当行为事件很少并不意味着风险低，而热线电话呼叫次数少也不意味着问题少 - 实际上，呼叫次数少很可能只意味着人们不信任这个系统。有的公司编制了与道德和合规培训相关的数据以及与知识和遵守行为准则相关的员工资质，但这种措施仍旧不够。

近年来，合规测量变得更加富有洞察力。有的公司则采取相对简单的衡量措施：衡量在公司的在线行为准则中哪些部分收到了反馈，这也有助于指示可能出现问题的环节。还有的公司追踪来自正常管理渠道的报告数量和类型，将其与热线电话的报告数量和类型进行对比。另有一些组织专注于所提问题的性质和类别、组织中的发起者，以及是匿名呼叫还是可以识别的呼叫。一些公司对个人申请报告进行跟进，以确定报告者的舒适水平及其对于流程的满意度。有的指标与关键绩效指标和关键风险指标相关联，实时仪表盘指示风险或事件需要直接关注的位置。此外，越来越多的公司开始跟踪社交媒体站点中的不当行为指标，针对与公司开展业务的相关方寻找可疑不当行为的报告并进行跟进。另外，内部合规审计也可提供对于不当行为和相关风险的更深入洞察力。

内部调查结果是任何公司都可采取的最重要指标之一 - 有时也被称为文化调查或风险文化调查。通常，调查文档以电子的方式发送至大部分组织员工甚至所有员工，调查的重点是企业文化。如果处理得当，便可提供有关组织的道德和完整性、沟通的有效性、不当行为的观察等方面的美好洞察力。关注焦点在于人们是否信任同事和管理人员、他们对同事和管理人员的行为所感受到的舒适度，以及在上报不当行为指标时的自由度。这些调查通常每半年或每年开展一次，尽管原始结果很重要，但较长时间范围内的趋势具有更大的相关性，特别是根据业务部门或其他分类进行分析时更是如此。借助这些信息，管理人员可以清楚地了解合规计划和相关沟通以及近期的改进措施是否真正在员工中产生了积极反响，以及哪些地方需要进一步的关注。

**技术。**的确，企业可以使用很多种不同的技术工具来支持自身的合规计划。但研究显示，很多公司的工具都是基础而独立的工具，因此导致合规方法“相对孤立”，阻碍了跨组织的沟通和有效性。一项研究发现，大多数受访者（79%）倾向于在合规活动中采用基本的桌面工具（如 Word、Excel 等），并将其作为主要支持工具，而仅有少数的受访者（45%）采用由主要软件供应商提供的综合 IT 解决方案。该研究“指出了企业在 GRC 方面所采用的一种分散式方法，也就是数据和合规活动中的可怕‘孤岛’，而这种方法会导致合规高管无法获得企业风险的整体视图。”<sup>vi</sup>

<sup>vi</sup> 《合规周刊》- PwC 的更广泛的视角；更好的绩效。2012 年合规状态研究。

借助更先进的技术资源，公司可以确保信息、沟通、报告和监测在整个企业范围内高效展开。此外，还可识别合规风险，同时制定相关程序、控制措施和问责制，进而建立一个集成式的合规流程。同样，这些技术还有助于政策生命周期管理人员创建、批准、维护、存储、监视和自动化任务。它们还有助于实施政策培训和宣传、调查以及相关的测试反馈。它们可帮助企业建立自动化工作流，针对管理者或监督者所需的行动进行职责定位以及跟踪活动，同时还支持向高级管理层进行查询。它们还可实现流程和信息检索的自动化，包括控制测试、调查、认证和监管报告。它们支持事件补救、事件跟踪、关键绩效指标以及与监管机构的互动。它们还可为信息沟通提供实时消息传递和报告，以便在整个管理层和合规职能部门使用，也可提供定制仪表盘，并能够针对特殊问题进行直接的深入分析。此外，它们还为高层管理人员和董事会提供有关不合规的原因、财务影响、缓解措施和控制风险的所需信息。

**全局式方法。**对此，我们曾有所提及，但它值得我们直接加以关注。当合规计划包含迥然不同的部分时，其通常无法发挥较好的作用。这是现实。若要真正有效，合规计划就必须包含正确的要素，这些要素紧密结合，形成完整、协调良好的整体。对于在全球运营的大型、复杂组织而言，这一点在概念上非常容易实现，但事实上却极其困难。

我们知道，高效的合规计划应建立在以诚信和道德价值观为基础的文化之上，同时由首席执行官的言行推动，由董事会的支持和监督提供支持。其他所有关键要素均以此为基础进行发散。

## 回报

对于大多数公司而言，合规成本在飙升，不合规事件也在增加，遭受灾难性失败的风险实实在在地存在。打造真正高效合规流程的目标是可以实现的。有的公司已经达成了这一目标，实现了相关的业务优势，流程和人员驱动着企业实现成功。达成这种目标需要我们集中注意力和精力，但却并非遥不可及。

## 关于作者

作为 Steinberg Governance Advisors, Inc. 的 CEO，Rick Steinberg 是国际公认的治理、风险管理和合规专家。他的工作是为大型跨国公司、大中型市场公司的董事会提供董事会职责、治理、风险管理、控制和合规方面的建议。此前，他是 PricewaterhouseCoopers 的资深合伙人兼公司治理咨询实践的领导者。此外，他也是 PwC 的风险管理和控制咨询实践创始人，同时担任其全球领导者。

Steinberg 主导编制了 Treadway 委员会赞助组织委员会 (COSO) 的两份里程碑式报告，即《*内部控制 - 集成框架 (Internal Control -- Integrated Framework)*》和《*企业风险管理 - 集成框架 (Enterprise Risk Management – Integrated Framework)*》，这两份报告被公认为高效内部控制和风险管理标准。他还撰写了很多其他广受好评的报告，包括《*企业治理和董事会 - 哪些最有效 (Corporate Governance and the Board - What Works Best)*》及其手册、《*审计委员会的有效性 - 哪些最有效 (Audit Committee Effectiveness - What Works Best)*》；他的最新作品是《*治理、风险管理和合规：它不能发生在我们身上 - 驱动成功的同时避免企业灾难 (Governance, Risk Management and Compliance: It Can't Happen to Us – Avoiding Corporate Disaster While Driving Success)*》。

Steinberg 的作品经常被财经媒体引用，他本人也不时出现在全国财经新闻节目中，是著名商学院的客座嘉宾。他还是世界大型企业联合会全球公司治理研究中心顾问委员会的成员，是开放合规和伦理集团行政顾问小组成员，此外还与他人联合创办了由 PricewaterhouseCoopers 和特拉华大学公司治理中心主办的董事大学。