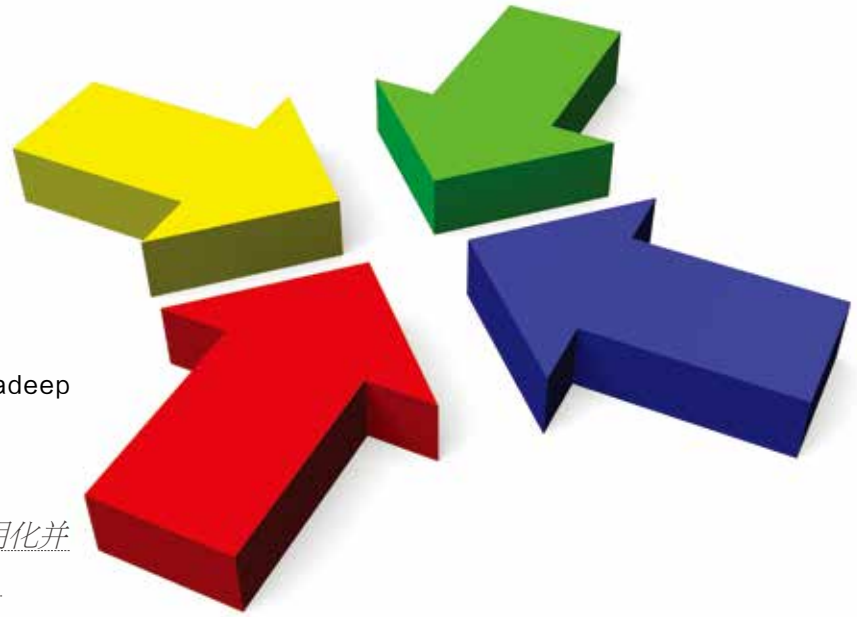
TECH PRACTICES



# 建立 IT 治理

## ESTABLISHING IT GOVERNANCE

Barry Nathan, CMA; Sean Hare; and Pradeep Raju, CMA
王宁 译，许可 校

*规范 IT 治理的关键是如何使 IT 治理透明化并且能够应对未知的安全风险和经营需求。*

专业的会计师现在都知道了解技术对他们在工作中的表现至关重要。人工智能、区块链、预测分析和自动化等新兴技术进入会计流程，改变了会计师的工作方式和工作职责。组织中的技术变革导致对现有 IT 系统和流程需要进行大量的再评估。任何此类的改变都应该通过 IT 治理来着手。

IT 治理的主要目标是通过自动化（有效性）和降低成本（效率）增加你的业务服务的价值，同时也要应对风险，确保结果与组织的总体战略方向一致。为客户和股东交付价值需要转化为成果。当然，你也需要考虑投资回报的问题。你当然不需要自己做这些选择。它需要一组流程、职责、角色、关系和一个规范的 IT 治理框架。

### 什么是 IT 治理?

ITIL 的 IT 服务管理流程和 IT 治理协会，以及 ISACA 都致力于提供一个指导性的组织架构。他们都把 IT 治理模式定义为能够有利于整个组织的 IT。IT 应该推动整个组织朝着战略性的目标前进，并通过技术支持来使之实现。这是技术与业务相一致的地方，反之亦然。IT 治理的核心是通过提供一系列的检察和平衡来帮助实现公司的战略。这些检查和平衡有助于确定正确的优先事项、评估风险、确保合规性和衡量绩效（平衡计分卡）。组织中的治理需要对责任制或问责制的应用、沟通、授权和监督。IT 治理也并没有什么不同。

### 责任制或问责制

公司的领导（通常是董事会）负责制定战略，并且确定组织的风险承受能力。公司的首席执行官（CEO）随后执行政策、标准，并且实施该战略。这包括对 IT 投资项目组合的开发和增加相关知识管理。首席信息官（CIO）要确保项目及时进行，并且通过强大的项目管理规章来满足预期的成果和成本，确保 IT 体系结构的标准化，并实现 IT 控制框架。

推进一个技术项目是一个组织的战略性商业决策，所有部门都应该有发言权。每个部门都应该表达出他们自己的 IT 需求。不管这些需求是项目上的、软件上的或者其他技术方面的，它们的目标都是满足其组织的目标。如果组织的所有成员都觉得自己有发言权，那么 IT 治理就会变得有条不紊，IT 团队知道如何使用有限的资源。

IT 部门也必须在公司管理中占有一席之地。它

将在评估如大型设施、服务器、网络、安全、数据存储及灾难恢复和业务连续性等基础设施影响的同时，考虑到项目的整体战略。在许多情况下，IT 部门还负责软件许可、软件和硬件的生命周期、计算机，以及无线通信和设备。升级还是采用新技术的决定将在所有这些领域产生影响。

## 沟通

每一方都应该准备好打开天窗说亮话，解释他们在技术上需要什么，为什么需要。他们需要展示 IT 采购流程如何使组织实现其战略目标。这些报告必须包括项目整个生命周期的投资回报率、净现值或者其他可接受的财务指标。部分费用还要包括处置、升级和重置成本。另外，还需要对与项目相关的风险进行全面的评估。陈述中还应提供项目管理需要、实施计划和 IT 基础设施需要的各种初步数据。

有一些公司会要求董事会成员参加报告会并提供一些指导性的建议。董事会成员会会充当中立的角色，来减少决策中的“政治”成分。项目的正式批准取决于该组织。一般来说，这个组织是执行团队、董事会和利益相关者的结合。如果董事会或委员会没有直接参与进来，则应该与他们沟通。 在这一点上，董事会应该批准这个项目的筹资和预算。董事会和管理人员应该进行整体的监督，以确保项目在必要时能够完成或停止。

## 授权

有些决定权应该留给 IT 部门。很多人认为如何保护软件是最重要的决定。IT 部门应该决定是自己开发软件还是购买软件，设置为平台即服务（as Platform as a Service，PaaS）还是托管在云系统中或者是两者的混合设置。这些都是 IT 部门在做决定时需要考虑的。

应该允许某个独立的部门来选择和管理自己的软件吗？一个良好的 IT 治理框架应该有 IT 部门参与其中，评估软件的安全性质量并且确定它是否是可接受的风险。IT 部门还需要知道为保证软件高效率运行所需要的网络和宽带要求。它应该管理技术，因为它在最有利的位置，知道和理解什么对组织是最好的。

## 监控

为了确保在业务活动、IT 活动和 IT 过程中进行持续性的改进，建立衡量标准是非常重要的。一些组织可以提供 IT 治理方面的相关信息。但是在 IT 治理方面，每一个组织都有自己的侧重点。

- ITIL 框架是一组最佳实践的框架结构，旨在将业务需求与软件资产管理、服务支持、服务交付、安全管理和应用管理相结合。
- 信息及相关技术的控制目标（Control Objectives for Information and Related Technology，COBIT）最初是由 ISACA 开发的，现在是由 IT 治理研究所（IT Governance Institute，ITGI）发布和维护。COBIT 有 34 个主要的控制目标。这些控制目标分成 4 个领域，具体为规划和组织、获取和实施、交付和支持，以及监控。每个目标都有不同程度的成熟度。
- ISO 17799 为 IT 安全实践提供监管。由于仅聚焦于安全性，人们通常不将它作为 IT 治理框架的来源。

IT 治理为组织提供了有效管理 IT 业务和技术项目的结构。对于一个组织来说，让每个人都来讨论他们的技术需求以及他们如何适应组织的战略目标是至关重要的。考虑到诸如风险、组织安全和经营影响等因素，该流程应该是可定义的、透明的、可复验的。这个过程越正式，结果就会越好，性价比也会越高。**SF**

**Barry Nathan**，CMA，美国俄勒冈州塞伦 Transportation Information Systems 的 Oregon 分部的财政经理（刚退休）。他也是 IMA 波特兰分会的会员。联系方式：barryn@prodigy.net。

**Sean Hare**，IMA 的 IT 和运营部副总裁。联系方式：share@imanet.org。

**Pradeep Raju**，CMA，美国俄勒冈州波特兰 Portland Public Schools 的业务和财务经理。他也是 IMA 波特兰分会的会员。联系方式：raju_pradeep@outlook.com。