COBIT 框架下企业 IT 治理的首要特征——以业务为中心

广州铁路职业技术学院　　刘红英
北京财贸职业学院　　周　梅

【摘　要】文章首先提出 IT 治理与 COBIT 的关系——COBIT 框架是业界常用的 IT 治理框架，并详细论证了 COBIT 框架下企业 IT 治理的首要特征——以业务为中心。以业务为中心的 IT 治理首要特征论述主要从企业业务需求决定 IT 信息标准，IT 治理的三个层次和业务目标与 IT 目标、企业信息标准间的映射关系三方面展开。

【关键词】IT 治理；COBIT；内部控制；业务

一、企业 IT 治理框架通用框架——COBIT

对于许多企业而言，支持其业务的信息与技术是企业最有价值的资产，尤其对于银行、证券等金融机构。企业管理层已经逐渐认识到保障 IT 价值、管理与 IT 有关的风险，增加对电子信息的控制已经成为公司治理的关键要素。IT 治理已经成为公司治理中的一个重要组成部分。价值、风险和控制构成了 IT 治理的核心。

IT 治理通常有五个关注领域：⑴ 战略整合：关注于业务战略与 IT 规划的联系；规定、保持和验证 IT 的价值建议，使 IT 运营与业务运营一致。⑵ 价值交付：在整个 IT 服务交付周期内实施价值建议，确保 IT 实现了预期的战略收益，并关注 IT 成本的优化，提出了 IT 的固有价值。⑶ 资源管理：对 IT 资源优化投资并适当管理，致力于知识共享和基础设施的优化部署。⑷ 风险管理：要求企业高级管理层具备良好的 IT 风险意识，清晰了解企业对 IT 风险的承担偏好，了解 IT 合规性要求，将企业所面临的显著 IT 风险透明化，并将 IT 风险管理的职责嵌入到组织结构中。⑸ 绩效测评：追踪并监控 IT 规划实施，在项目终结、资源使用、流程绩效、服务支付过程中使用 IT 平衡记分卡。IT 平衡记分卡将 IT 战略转化为措施，这些措施可以实现传统财务管理方面无法测量的目标。

这些 IT 治理关注领域描述了高级管理层在企业内进行 IT 治理时必须考虑的重要因素。运营管理层利用 IT 流程来组织和管理日常的 IT 活动。要实现 IT 治理还需要融合实务界的最佳实践并将其标准化，以形成一个 IT 治理框架。该框架可以满足并支持那些广为接受的公司治理、风险管理的控制框架。

COSO（及类似框架）通常作为企业的内部控制整体框架，而 COBIT（信息及相关技术控制目标，Control Objectives for Information and Related Technology）则是业界常用的 IT 治理框架。COBIT 的最佳实践代表了业界专家的一致意见，并已被美国等 180 多个国家和地区普遍认可和广泛应用。COBIT 正在成为 IT 治理领域事实上的国际标准。

COBIT 的基本原理是：企业的业务需求推动投资 IT 资源，IT 资源被应用于 IT 流程，IT 流程交付有商业价值的电子企业信息，这些企业信息响应了企业特有的业务需求。因此，企业需要采用一套系统化的 IT 治理框架来投资、管理和控制 IT 资源，来确保其为企业提供信息服务。高度相关的管理和控制信息是 COBIT 框架的核心。

使用 COBIT 框架作为企业 IT 治理框架的优点还在于：⑴ COBIT 以业务为中心，使 IT 与业务始终保持一致；⑵ COBIT 为管理层提供了一个更好的 IT 视角；⑶ 在流程导向的基础上，COBIT 清晰界定了流程的所有者关系和职责；⑷ COBIT 采用通用的语言，容易被所有的利益相关方理解，易于被第三方及监管机构接受；⑸ COBIT 满足了 COSO 对于 IT 相关企业内部控制的要求。

二、COBIT 框架 IT 治理的首要特征——以业务为中心

COBIT 框架下，IT 治理的主要特点有：以业务为中心、以流程为导向、以控制为基础、以绩效测评为驱动。其中，以业务为中心是企业 IT 治理的首要特征。IT 治理的这个首要特征可以从以下三方面集中体现。

㈠ 业务需求决定 IT 信息标准

为满足业务目标，由企业 IT 系统提供的信息必须符合一定的控制标准，称为企业信息的业务需求。基于一个更广泛的质量、可信度和安全等要求，COBIT 定义了七个相对独立，但内涵又相互关联的信息标准，即企业信息的七个业务需求。这七个信息标准分别是：⑴ 效果：涉及到信息与业务流程相关程度的属性，以及信息交付的及时性、正确性、一致性和可用性。⑵ 效率：通过优化（生产率最高且符合经济效益）资源使用来提供信息。⑶ 保密性：保护敏感信息，避免未经授权的信息披露。⑷ 完整性：与信息的准确度和完全性有关的属性，与业务价值和预期相

一致，没有遗漏重要的或必须的信息。(5) 可用性：与业务流程对信息的当前或未来可用性相关的属性，也包括所需资源和相关能力的安全性。(6) 符合性：涉及业务流程与所需遵守的法律、法规和合同约定之间的符合程度的属性，即外部的强制要求和内部政策的遵循性。(7) 可靠性：为管理者提供可靠的信息，运营相关实体并履行所赋予的职责。

(二) 三个 IT 治理层次

企业 IT 治理以业务为中心的首要特征可以从 COBIT 框架下的三个 IT 治理层次来充分体现。

第一层是高级管理层及董事会。他们主要关注如何履行自身职责，主要使用“COBIT 董事会 IT 治理简介 (第二版)”等文件规范来理解 IT 控制的重要性、主要存在问题及他们的管理职责。

第二层是业务和技术管理层，及 IT 治理层。他们主要关注企业如何进行 IT 控制绩效测评、企业如何与其他同行进行比较？企业如何及时进行改进？主要使用 COBIT 中的管理指南和成熟度模型来分配职责、测量绩效、基准管理和阐述企业的能力差距。

第三层是从事治理、保证、控制和安全的专业人员。他们主要关注：企业 IT 治理框架是什么？企业如何实施 IT 治理框架？如何在企业内评估 IT 治理框架？本层人员主要使用 COBIT 及 VAL IT 框架、控制目标和关键的管理层实践来建立和完善企业的 IT 控制框架，通过“计划与组织 (PO)”、“获取与实施 (AI)”、“交付与支持 (DS)”“测量与评价 (ME)”4 个 IT 控制过程域和 34 个 IT 控制流程来组织 IT 控制目标和最佳实践，并将它们与企业需求联系起来。依靠“IT 控制实践第二版”、“COBIT 控制实践指南第二版”等文件规范来实施 IT 治理框架，通过“IT 保证指南”在企业内部评估 IT 治理框架。

COBIT 的基本特征之一是控制为基础，该框架依次在三个层次上制定了控制目标及其对应的测量指标。第一层次：IT 目标和指标，定义了业务对 IT 的期望和如何测评；第二层次：流程目标和指标，定义了 IT 流程为了满足 IT 目标必须交付的服务和如何进行评估；第三层次：活动目标和指标，确定为达到所需性能而采取的流程内活动以及如何测评。在此目标和测量指标体系中，活动层次上的测量指标驱动了流程层次上的控制目标，而流程层次上的测量指标驱动了企业业务对 IT 的总体期望目标。

(三) 业务目标与 IT 目标、企业信息标准之间的映射关系

COBIT 信息标准在为定义业务需求提供一个通用方法的同时，也制定了一系列一般业务目标和 IT 目标，作为与业务相关的、更加细化的基础用以建立业务需求和制定这些目标的衡量指标。企业利用 IT 来激发业务动力，也可以称之为“IT 的业务目标”。

在 COBIT 框架中，常用一个矩阵描述企业一般业务目标和 IT 目标，以及他们是如何映射到信息标准的，简化的矩阵如表 1 所示。

表 1 提供了一个阐述通用业务目标和 IT 目标、IT 流程和信息标准之间对应关系的整体视图，该视图可以用来指导企业如何确定具体的业务要求、目标和衡量指标，现举例阐述：

首先，由业务目标映射到 IT 目标。比如，对于基于财务视角的业务目标“(2) 管理 IT 相关业务风险”，该业务目标所对应的 IT 目标有 8 个，分别是 2- 响应符合董事会方向的管理需求、14- 登记和保护所有 IT 资产、17- 保护 IT 目标的达成、18- 清楚源自 IT 目标及资源的风险对业务的影响、19- 确保关键和机密信息与不应该访问的人相隔离、20- 确保自动化的业务交易和信息交换是可信的、21- 确保 IT 服务和基础设施能适当抵御和恢复因失误、恶意攻击和灾难而导致的故障、22- 确保因 IT 服务中断或变更而对业务的影响的最小。该业务目标主要通过审查 COBIT 信息标准中的 3- 保密性，4- 完整性和 5- 可用性三项来提供合理保证。

其次，由 IT 目标映射到 IT 流程。如 IT 目标“19- 确保关键和机密信息与不该访问的人相隔离”所对应的 IT 流程分别是：PO6- IT 投资管理、DS5- 确保系统安全、DS11- 数据管理和 DS12- 物理环境管理。

再次，通过 IT 流程 IT 目标之间的反向映射关系获得反馈与修订。如规划与组织过程域中的第六个控制流程“PO6- IT 投资管理”就与 28 个 IT 目标中 3 个 IT 目标存在反向映射关系。这三个 IT 目标分别是：12- 确保 IT 成本、收益、战略、策略和服务等级的透明度和被理解；24- 提高 IT 成本效益和对业务收益的贡献；28- 确保 IT 具有基于成本效益的服务质量、持续改进和对未来变化的准备。IT 控制人员、内审人员等可以从以上三个 IT 目标分别评价和完善 IT 控制流程。

最后，综合权衡 IT 目标与 IT 流程。值得注意的是：IT 流程与 IT 治理的五大关注领域、COSO 内部控制整体框架、COBIT 的 IT 资源和 COBIT 信息标准等都存在重要的映射关系。如 34 个 IT 治理流程中的“PO5- IT 投资管理”流程，在计划与组织过程域中的重要性为 M (中等)。PO5 主要关注 IT 治理五大领域中的“价值交付”领域，其次是“战略整合”和“资源管理”两领域。PO5 最主要关注 COSO 中的“控制活动”方面，其次是“监控与评价”和“风险评估”两环节。同时，PO5 又涉及“应用系统”、“基础设施”和“人员”这三种 IT 资源。PO5 主要关注 COBIT 信息标准中的“效率”和“效果”，以及“可靠性”。

因此，IT 治理人员在实施企业 IT 治理框架过程中要通盘考虑以上影响因素，帮助企业的业务管理层和董事会期望获得较好的 IT 投资回报，满足业务需求以增加利

表 1　企业业务目标、IT 目标与 COBIT 信息标准间的映射关系

	业务目标	IT 目标	COBIT 信息标准
财务视角	(1) 为 IT 保障业务投资提供良好的投资回报	24	2- 效率
	(2) 管理 IT 相关业务风险	2,14,17,18,19,20,21,22	3- 保密性,4- 完整性,5- 可用性
	(3) 改进公司治理和透明度	2,18	7- 可用性
客户视角	(4) 改善客户倾向和服务	3,23	1- 效果
	(5) 提供有竞争力产品和服务	5,24	1- 效果,2- 效率
	(6) 建立持续和可用的服务	10,16,22,23	1- 效果,5- 可用性
	(7) 对业务需求变更,提供灵活快捷的响应	1,5,25	1- 效果,2- 效率
	(8) 完成服务交付的成本最优化	7,8,10,24	2- 效率
	(9) 为战略决策提供可靠的和有用的信息	2,4,12,20,26	1- 效果,4- 完整性,7- 可靠性
内部管控视角	(10) 改善和维护服务流程的功能	6,7,11	1- 效果,2- 效率
	(11) 降低流程成本	7,8,13,15,24	2- 效率
	(12) 提供与外部法律、法规及合同的合规性	2,19,20,21,22,26,27	3- 保密性,6- 符合性
	(13) 提供与内部政策的符合性	2,13	3- 保密性,6- 符合性
	(14) 管理业务变更	1,5,6,11,28	1- 效果,2- 效率
	(15) 改善与维持运营和员工生产力	7,8,11,13	1- 效果,2- 效率
成长视角	(16) 管理产品和业务创新	5,25,28	1- 效果,2- 效率
	(17) 获得和维持技能熟练的与上进的人	9	1- 效果,2- 效率

注：为节省篇幅，表 1 中业务目标所对应的 IT 目标只给出序号，这 28 个 IT 目标的具体描述等相关内容，读者可参阅 COBIT4.1 版相关文档。

益相关方的收益；在隐私保护和金融报告领域，以及财政、药品和卫生保健部门，要求 IT 控制满足有关的合规性要求，如萨班斯法案等；选择符合成本效益原则的服务提供商、管理服务外包和采购；更加负责的 IT 相关风险，如网路安全；采用控制框架和最佳实践，以监控和改进关键 IT 活动，进而增加业务价值，并降低业务风险；尽可能通过遵循标准的而非特别制定的方法来满足优化成本的要求等。●

【参考文献】

[1] 陈婉玲，杨文杰. ISACA 信息系统管理准则及其启示 [J]. 审计研究，2006 (增刊).

[2] 王海林.IT 环境下企业内部控制探讨 [J]. 会计研究，2008 (11).

[3] (美) 詹姆斯·A·霍尔 (James.A.Hall). 信息系统审计与鉴证 [M]. 李丹，刘济平译.北京：中信出版社，2003.

[4] IT Control Objective for Sarbanes- Oxley (萨班斯 - 奥克斯利法案的 IT 控制目标)：The Role.