COBIT及其应用问题的理论研究

陶黎娟　庄明来(博士生导师)

(厦门大学　厦门　361005)

【摘要】本文在介绍信息及相关技术的控制目标的最新版本COBIT4.1的基础上,从综合性、系统性、过程导向和理论价值方面分析了COBIT的特征,同时指出了COBIT存在的问题,最后提出了COBIT未来研究应关注的问题。

【关键词】COBIT　COSO框架　IT治理

信息及相关技术的控制目标(COBIT)是由信息技术治理协会提出的IT内部控制框架,该协会于1996年、1998年、2000年、2005年分别颁布了COBIT1.0、COBIT2.0、COBIT3.0以及COBIT4.0,2007年5月,版本更新到COBIT4.1。在这个过程中,COBIT已从审计师的审计工具演变为IT内部控制框架,越来越多地被IT管理人员使用。

一、COBIT的特征

1. COBIT是COSO框架的补充框架。COBIT作为COSO框架的补充框架已被广泛认可。大多数国际组织在采纳COSO框架时,同时使用了COBIT控制标准。目前,几乎所有大型的国际会计公司均已采用COBIT,或在评价内部控制时至少采用了该框架中的主要概念。2005年,欧盟决定选择COBIT作为其审计准则。

2. COBIT体现了系统思想。从整体的角度全面评估企业过程的方法被称作系统思考法,系统思考法将组织看做许多过程相互作用以实现绩效的复杂网络。全面分析企业过程,就要求我们在分析每一过程时,必须充分考虑该过程所在的环境、该过程与执行人员和组织的关系,以及该过程对上下游活动的影响(O'Donnell,2005)。

对于每一过程,COBIT都提供了该过程所影响的IT信息标准、利用的IT资源和该过程所属的IT治理领域,并给出了过程对应的RACI图。RACI图描绘对于某项具体活动(实现具体控制目标的行为),组织中的各个角色(如CEO、CFO、业务经理、CIO等)分别负有何种职责(报告的责任、被咨询的责任、被告知的责任)。COBIT还提供了每一过程所涉及的输入与输出。

参照COBIT的过程框架,利用RACI图可以更好地理解不同人员在该过程中的责任和义务。过程目标无法顺利实现时,可以根据RACI图找到相关负责人,从而追根溯源,更及时地发现和解决问题。另外,IT内部控制系统中各个过程之间相互作用、相互影响,某一过程的失误未必源自该过程本身的执行不力,而是有可能源自其他相关过程。在考核过程绩效时,可以依据输入输出图,依次排查有关人员在相关过程中的责任履行情况,更准确地发现问题所在。因而,COBIT作为一整套系统模型,为企业组织各种IT资源、权衡各个过程之间的输入输出关系、全方位进行IT内部控制和审核、实现IT对企业战略的切实支持提供了基础框架。

3. COBIT的过程观点。COBIT过程模型按照生命周期法将企业的IT活动划分为计划与组织、获取与实施、交付与支持、监督与评价四个域,四个域又包括34个处理过程,每个过程均有要实现的整体控制目标和若干具体目标,对于具体目标还有相应的审计指南。COBIT既易于实施又具有一般性,从而适用于不同类型的审计。作为一个过程导向的框架,COBIT可以使IT审计人员和控制人员更容易地了解企业的IT内部控制的现状,找出薄弱环节,并提出改进建议。

4. COBIT概念模型具有内部一致性。COBIT最初被管理者看做是IT内部控制的基本工具。由于COBIT对内部控制的强有力关注,内部审计人员和外部审计人员均将其应用于财务报告审计、经营和合规审计(Tuttle和Vandervelde,2007)。作为IT内部控制框架,COBIT概念模型涉及IT过程、IT资源和信息标准三个因素,虽然在实务中得到广泛运用,但其是否合理并未得到理论验证,为此Tuttle和Vandervelde(2007)采用实证研究的方法,检验由IT过程、IT资源、信息标准三因素组成的COBIT概念模型的内部一致性。实证研究要求12名IT审计人员评价7个信息标准和4个IT资源的重要程度,据以计算COBIT概念模型自身所反映的各个过程的风险程度的数值。另外,再由29名审计人员(12名IT审计人员和17名非IT审计人员)对34个过程的风险程度评分。对得出的两个过程的风险程度构建线性回归模型,笔者发现两个变量显著相关,证明COBIT作为IT内部控制框架,其概念具有内部一致性,从而认定COBIT在IT内部控制和审计领域是一个有效框架,这在理论上为COBIT用于IT内部控制提供了支持。

二、COBIT存在的问题

1. COBIT对于具体操作问题涉及不多。COBIT融合了IT治理领域的若干模型、工具和框架,这也使其未能包括各个层次的具体操作指南和实施步骤。COBIT是一个控制框架,而非具体过程框架,COBIT从战略、战术、运营层面给出了对IT内部控制系统的测评、审计方法,面对众多具有不同需求的用

户，为了实现可实施性和可理解性，其内容必然丰富、广泛但无法深入。总体来看，COBIT涉及范围广泛，但在某些方面缺乏具体的操作步骤和指南。事实上，由于目前已经颁布了许多被广泛接受的国际标准，从而COBIT也没有必要再面面俱到。为了更好地进行IT治理，参照COBIT的一系列映射，企业可以综合使用多个模型、工具和框架，从而实现全方位的IT治理。

2. COBIT是一个定性框架，缺乏定量描述。COBIT框架解释了34个IT过程如何提供实现企业目标所需的信息。Tuttle和Vandervelde（2007）的实证研究表明，把COBIT作为一个IT内部控制和审计框架，信息系统的审计人员并非对所有过程予以同样的关注，甚至有7个过程几乎没有受到特别关注。而COBIT并未给出各个过程的相对重要程度。为了解决这个问题，S.J Hussain和M.S Siddiqui（2005）以COBIT过程模型为基础，参照各个过程涉及的IT资源和影响的信息标准，计算出四个域的权重矩阵，构造了COBIT的量化扩展模型。通过对该模型的运用，企业可以计算和衡量COBIT框架中不同域和过程的影响度。另外，COBIT框架侧重于“控制”，虽然设置了成熟度标准，但是都是定性的描述性语言，没有给出判断成熟度的明确指标，无法用于量化评估。这就导致了在实际运用中尤其在进行评审时，难免因审计人员的个人素质造成审查结果的偏差。

3. COBIT概念模型值得进一步探讨。Tuttle和Vandervelde（2007）采用探索性因子分析法对COBIT概念模型涉及的4个IT资源、7个信息标准进行分析，发现它们并未严格按照类别划分为IT资源和信息标准两个维度。在信息系统的审计人员的认识中，它们实际上代表着三个不同的因子，第一个是由可靠性、保密性、完整性和效率组成的因子，笔者称之为“信息质量因子”，即以有效率的方式保证信息的可靠、保密和完整；第二个是由符合性、人员、有效性和数据组成的因子，笔者称之为“IT处理过程”，即对法律、法规和契约的有效遵循受人员的影响并且需要获得必要的数据；第三个是由可用性、应用软件、基础设施组成的因子，笔者称之为“IT设计因子”，即有关IT设计的因素（应用软件、基础设施）确保企业所需的信息是可用的。综合以上三个因子，就构成了IT环境下的内部控制模型。由于会计和信息系统领域缺乏一种经证实的有关内部控制有效性决定因素的理论，从而笔者希望这个研究结果是一个探索性的开端，这为我们进一步研究COBIT的合理性指明了方向。

三、COBIT的应用研究

COBIT自产生以来，就在内部审计领域发挥着越来越重要的作用。Ridley等（2004）通过ProQuest数据库和google网站搜索有关COBIT的文章，并按文章所提供案例的实务/学术导向、应用/理论导向将其分类，最后发现只有不到10%的文章属于学术导向，90%多的文章都属于实务导向。另外，笔者发现实施COBIT的企业中，53%属于大型企业，15%属于中小型企业，32%无法判断企业规模。对于COBIT的实施水平来讲，24%的企业达到了高水平，21%的企业达到中等水平，50%的企业为低水平，其余企业的实施水平未知。实施COBIT的企业中，44%属于美国企业，21%属于亚洲/澳洲企业，21%属于欧洲企业，9%属于非洲企业，其余的未知。在若干行业中，金融类企业实施COBIT的居多。

在我国会计界，大多数学者对COBIT的研究仍以介绍和借鉴为主（刘汝焯，2000；陈婉玲、袁若宾，2006；王德禄，2006），或者对各个IT治理工具进行比较（李维安、王德禄，2005；甄阜铭，2007；苗连琦，2008），或者探讨COBIT在信息系统审计与内部控制（陈志斌，2007；金文、张金城，2005）、IT治理（饶艳超，2003；唐志豪，2008）等方面的作用以及对我国的影响等，也有文章涉及案例。总体来讲，对COBIT运用情况的研究较少，对运用效果的研究更是少之又少。由于我国正处于信息化发展初期，对COBIT的整体运用和借鉴层次也相对较低。大型企业和金融类企业的信息化程度较高、IT治理更加复杂，组织对IT内部控制更加感兴趣，因此可以合理预见，在我国对COBIT的借鉴和运用同样以大型企业和金融类企业居多。同时，由于COBIT是舶来品，跨国企业更容易实施。因此，未来研究可以关注COBIT实施企业的范围和特征以及实施层次和结果。对这类问题的研究具有实际意义：如果能够确定COBIT的实施会提高IT治理效果，那么通过分析成功和不成功的实施案例，就可以更好地理解最佳实践；另外，通过分析实施COBIT的企业或行业的分类情况、地域情况等，也可以确定不同组织对IT投资的不同需求，从而更科学地支配有限的财力。

四、结语

COBIT是一个非常值得借鉴的信息系统评审和信息化建设的指导框架，是考察信息化建设过程的一个重要参照体系。作为一种先进的IT治理工具，我们有必要借鉴，但是应该注意到我国还处于信息化发展初期，COBIT的实施层次和实施成本是必须考虑的问题。另外，COBIT虽然是一个既有的国际通用标准，但正如Tuttle和Vandervelde（2007）的研究结果所揭示的，这并不表明其本身是完全科学的，在用于IT内部控制和审计时，其概念模型有待改进。因此，我国学者在对COBIT进行研究时，一方面要注重“本土化”研究，另一方面要注重“评判式”研究，在引入借鉴时，不能满足于对COBIT进行简单删减和借鉴，同样应该加强对IT内部控制和审计、IT治理的理论研究，对COBIT进行有意义的改进，争取走在世界前列。

【注】 本文系教育部人文社会科学重点研究基地重大项目（项目批准号：06JJD630019）阶段性成果。

主要参考文献

O´Donnell, E. Enterprise risk management：A systems－thinking framework for the event identification phase. International Journal of Accounting Information Systems，2005；6