构建适合我国企业的IT控制实施标准体系研究

池国华　关建朋

2010颁布的《企业内部控制应用指引第18号——信息系统》(以下简称《信息系统指引》)是目前我国企业实施IT控制最重要的规范。然而该指引侧重于原则式指导，作为操作依据来讲，内容不够具体，没有根本解决IT控制“实施难”的问题。因此，笔者拟通过借鉴COBIT(Control Objectives for Information and related Technology)框架，对构建适合于我国企业的IT控制实施标准做些研究探讨。

一、借鉴COBIT框架进行IT控制的可行性分析

COBIT框架是当前最为全面和成熟的IT控制框架，其要求的适用环境及条件也最为严格。COBIT依赖于较高的信息技术水平和较完善的内部治理结构。一个信息化水平低、公司治理不健全的企业，投入高昂成本以采用COBIT，其结果必然是得不偿失的。因此，在信息化程度和公司治理尚待发展的情况下，我国不适宜直接采用COBIT标准。那么对其进行合理借鉴并结合我国《信息系统指引》进行IT控制是否可行呢?

这就需要首先比较分析《信息系统指引》与COBIT框架的异同。显然，COBIT篇幅巨大，体系完整独立，单在内容总量上讲，两者并不具可比性。但《信息系统指引》基于系统生命周期设计的流程控制点逻辑完善，可与COBIT关注的IT流程进行比较，以发现优势或不足。图1列示了COBIT的IT流程与《信息系统指引》流程关注点的关联状况。

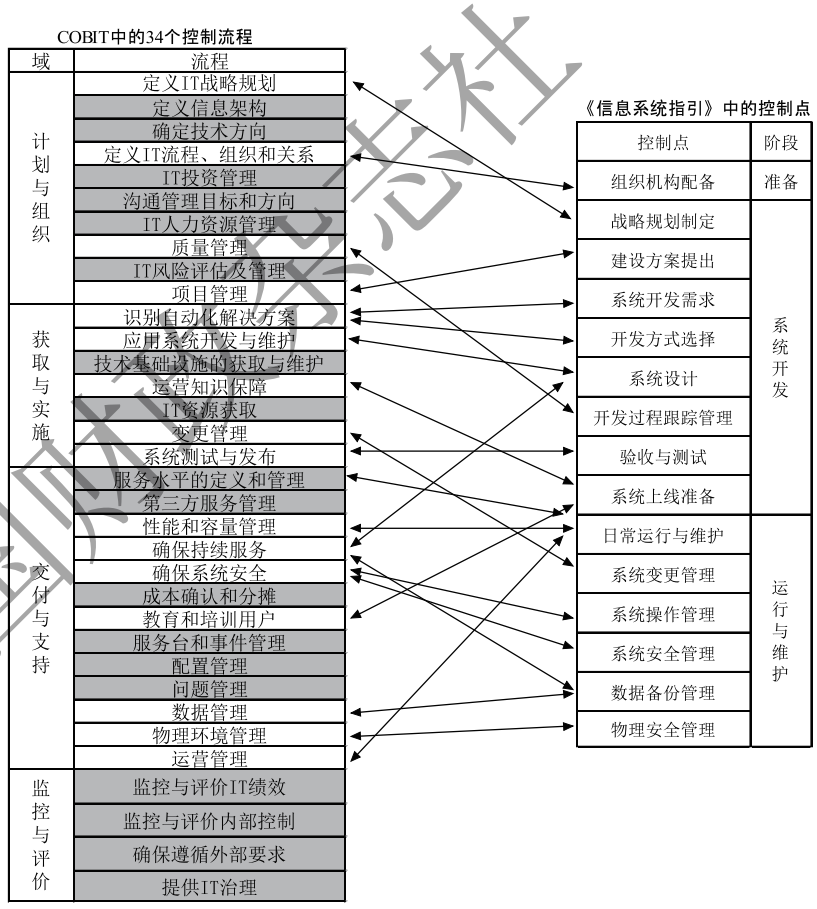

图1　COBIT与《信息系统指引》流程关注点的关联

通过流程点的对比，可以看出：第一，《信息系统指引》所涉及的控制点都能在COBIT的IT流程中找到对应，比如COBIT“定义IT战略规划”流程涉及如何制定战略规范，即涵盖了“战略规划制定”这一控制点。而COBIT中的某些流程，并未在《信息系统指引》的控制点中找到对应，如“问题管理”、“第三方服务管理”等。第二，《信息系统指引》的控制点设计侧重于系统开发、运行和维护阶段，而COBIT对系统项目前期的“计划与组织”也给予重视，在控制点设计方面也更加细化和全面，比如关

表1　　基于COBIT框架的IT流程和风险点设计

域	流程	风险点
计划与组织	定义IT战略规划	战略规划风险
	定义信息架构	信息架构风险
	确定技术方向	技术设计风险
	定义IT流程、组织和关系	IT流程、组织与关系风险
	IT投资管理	IT投资管理风险
	沟通管理目标和方向	管理目标和方向沟通风险
	IT人力资源管理	人力资源管理风险
	质量管理	质量管理风险
	IT风险评估及管理	风险评估风险
	项目管理	项目管理风险
获取与实施	识别自动化解决方案	自动化方案设计风险
	应用系统开发与维护	系统开发与维护风险
	技术基础设施的获取与维护	IT基础设施风险
	运营知识保障	运营知识保障风险
	IT资源获取	IT资源获取风险
	变更管理	变更管理风险
	系统测试与发布	系统测试风险
交付与支持	服务水平的定义和管理	IT服务水平管理风险
	第三方服务管理	第三方服务管理风险
	性能和容量管理	性能和容量管理风险
	确保持续服务	持续服务风险
	确保系统安全	系统安全管理风险
	成本确认和分摊	IT成本分摊风险
	教育和培训用户	用户培训风险
	服务台和事件管理	服务台和事件管理风险
	配置管理	配置管理风险
	问题管理	问题管理风险
	数据管理	数据管理风险
	物理环境管理	物理环境管理风险
	运营管理	运营管理风险

注“信息架构”、“技术方向”等基础性工作。第三，COBIT将“监督与评价”作为一个独立的活动域，并设计了相应的IT流程，而《信息系统指引》单纯围绕信息系统的整个生命周期环节进行设计控制点，并未涉及独立的监控及评价。究其原因，主要在于《信息系统指引》是作为整个内控规范体系的一部分，监控及评价的内容由其他应用指引和评价指引进行规范；而COBIT却是一个独立完整的框架。

由上可以得出一个推论：我国企业如果基于COBIT的34个IT流程进行控制，也将满足《企业内部控制基本规范》和《信息系统指引》对信息系统控制的要求，能够达到合规性目标。

二、构建我国IT控制实施标准的路径分析

IT控制实施标准，是指企业实施IT控制的具体依据或操作指南，是对《信息系统指引》的细化。建立IT控制实施标准具有重要的现实意义。一方面，IT控制实施标准强调通过在内部控制整体实施过程中强化IT控制，而非独立实施IT控制的各个环节，有助于节省资源投入提高控制效率；另一方面，IT控制实施标准也可作为内部控制评价中IT控制评价部分的具体标准，有助于解决我国企业目前IT控制评价难的问题。

需要注意的是，本文提出的“IT控制实施标准”是一个相对狭义的概念。COBIT既是一个IT控制框架，也是IT控制的标准。但是本文所设想的“IT控制实施标准”远没有COBIT框架的内容丰富，其逻辑结构也没有像COBIT那样复杂。IT控制实施标准试图解决的是在内部控制实施过程中如何强化IT控制的问题，主要围绕IT风险的应对进行。框架式研究IT控制虽有必要，但并不是本文的重心。

当前，理论界和实务界普遍认为基于业务流程控制风险的方式最为有效和实用。我国现行企业内部控制规范指引强调通过梳理业务流程，找准关键风险点，进而采取有效措施加以应对。IT控制的实施过程也应当通过关注IT流程，识别潜在IT风险，进而采取措施对IT流程加以控制。具体来讲，IT控制实施标准应当解决以下几个问题：①IT流程。企业IT活动存在哪些必要的流程。②风险点。企业该主要关注哪些风险。③风险迹象。这些风险存在什么样的迹象，怎样识别。④风险级别。为分配控制资源，风险的级别或重要程度如何确定。⑤控制措施。针对风险基本的控制措施是什么。

三、我国IT控制实施标准体系的内容构成

表2　　流程成熟度与风险级别对应表

成熟度级别	0级无级别	1级初始级	2级可重复级	3级定义级	4级可管理级	5级优化级
风险级别	高风险/不适用	中至高风险	中风险	低至中风险	低风险	基本无风险

表3　　战略规划风险级别一览

流程：定义战略规划	
风险：战略规划风险	
风险级别	定义
高风险/不适用	①未实施IT战略规划。②管理层也未意识到IT战略规划的必要性。
中至高风险	①IT管理层已经认识到战略规划的必要性，但只有在针对特定业务需求时才进行必要的规划。②IT战略规划偶尔会在IT管理层会议上进行讨论。③业务需求、应用和技术的一致性只是偶尔被动发生。④企业仅仅依据特定项目非正式地识别IT战略风险。
中风险	①业务管理层仅仅在必要时才与IT管理层一同制定IT战略规划。②规划在管理层要求时才做更新。③战略决策依据每个项目来驱动，不能与企业整体战略保持一致。④对战略决策风险的识别依靠直觉。
低至中风险	①制定了何时及如何实施战略规划的相关政策。②IT战略规划遵循书面的结构化方法。其编制流程合理，也能保证规划工作正常实施，但在具体的实施过程中却要依靠个别管理者的判断，且缺乏后续检查方法。③财务、技术及其人力资源策略对IT战略的影响日益增加。④业务管理层的会议上会讨论IT战略规划。
低风险	①IT战略规划的编制已成为一项标准化活动，同时管理层意识到IT战略规划存在例外情况。②战略规划纳入高级管理层的工作职责。IT战略规划流程得到有效监控，其有效性能得到有效测量。IT战略规划涵盖长、短期IT计划，并能逐层向下分解。③IT战略和企业战略能保持一致。④制定了系统开发和运行中使用内、外部资源进行决策的流程。
基本无风险	①IT战略规划存在正式文件，是一个可调整的过程。②企业极其重视IT战略规划，并通过对IT投资来实现业务的价值。③在规划过程中，能不断更新对IT风险的考虑。制定并持续更新长期IT计划，以便满足技术和业务的变化。④制定了遵循行业规范的相关标准，并纳入到战略规范化流程之中。⑤IT战略规划也包括如何开发新技术以驱动业务创新，从而提高组织的竞争优势。

综上所述，笔者认为可以从以下五个方面构建我国IT控制实施标准体系。

（一）IT流程

IT流程的设计应当遵循信息系统的生命周期理论。我国《信息系统指引》也是按照这一科学思路，对信息系统控制的各个要点进行了规范。然而，不无遗憾的是，《信息系统指引》只是提纲式的泛泛约束，缺少更具体的实施要求。相比之下，COBIT体系更完备，实施操作性更强。但值得注意的是，COBIT划分的域中包含“监控与评价”，并涉及4个IT流程，即“监控与评价IT绩效”、“监控与评价内部控制”、“确保遵循外部要求”和“提供IT治理”；如果将它们也作为IT控制实施标准中IT流程的内容，那么势必将与我国《企业内部控制评价指引》的实施存在或多或少的冲突。因此，除“监控与评价”域的IT流程外，COBIT关注的其他流程，应当纳入控制点的范围。具体见表1。

（二）风险点

我国内部控制制度体系始终贯穿着风险管理理念，每一处控制点都对应着相应风险，以做到有的放矢。在COBIT框架中，并没有直接提及风险点的问题，但实际上也隐含着风险管理的理念。COBIT通过制定信息标准与控制目标来规范相应的流程控制，显然这正是一个应对潜在不确定性、控制IT风险的过程，或者说，COBIT流程控制背后都对应着一类风险。因此，对于IT控制实施标准中风险点的设计，笔者将每一个流程中潜在的诸多风险归为一类，比如“定义IT战略规划”对应“战略规划风险”；这样依次共设计了30个风险点，具体见表1。

（三）风险迹象

风险迹象是风险存在的外在表象，是识别风险的关键。如何确定风险迹象呢？COBIT框架中每个流程设定的控制目标，为本文提供了一个很好的思路。控制目标一方面对应了IT流程的具体内容，另一方面指明了该流程优化所需要努力的方向。因此，我们可以据此来判断该流程控制是否已经完善，是否仍存在风险。受篇幅所限，本文仅以“定义战略规划”流程为例，说明其风险迹象的设计过程。该流程的控制目标包括IT价值管理、IT与业务的一致性、当前能力和绩效的评估、IT战略规划编制、IT战术计划和IT项目组合管理六个方面，那么该流程的风险即可从以下六方面去判断：

1.战略规划是否充分考虑了IT价值。如果在战略规划中对IT价值考虑欠缺，由此可能导致IT投资不能带来相应的效益。

2.IT是否能满足业务需求，并保持持续的一致性。在IT项目的战略规划过程中，如果未能充分掌握业务的需求状况，盲目开发或者上马系统，将可能造成系统功能与业务需求不相一致，限制IT功能发挥甚至阻滞业务活动。

3.战略规划过程中是否对IT开发的现有能力进行充分评估和掌握。企业要

开发一套IT系统，在战略规划阶段必须对系统所能实现的能力和效果进行评估，以便与业务的实际需求进行比较，进而判断可行性。如果未对IT解决方案有充分了解，极可能与业务需求不匹配而导致投资损失。

4.战略规划编制是否有严格流程，并得以执行。战略规划编制如果未能严格执行，可能因忽视其他利益相关方的需求，而导致后续项目执行困难。

5.是否存在配套完善的战术计划。如果缺少详细的与战略规划相一致的战术计划，可能导致IT战略执行过程中出现混乱，不能实现预期目标。

6.战略规划是否充分考虑了投资项目的组合管理。对于同期内的多个项目，如果不能进行有效的项目组合管理，对资金分配、授权、职责等问题加以明确，将影响项目的有序实施，由此产生一系列不利影响。

当然，该六个方面只是提供了观察风险迹象的角度，并不能穷尽所有情况，具体操作仍需要相关人员的专业判断。

（四）风险级别

风险级别是衡量风险大小的指标，通过界定风险级别可以确定应对的优先次序。本文将借鉴COBIT的成熟度模型来确定风险级别。成熟度级别越低，那么该流程的完善度也越低，风险也就越高；成熟度级别越是接近优化级，那么该流程的风险就越低，具体见表2。

每一个IT流程都对应一套成熟度模型，本文仍仅以“定义IT战略规划”流程为例进行说明，详见表3。

风险级别的判定同样依赖于专业人员的主观判断。一个IT流程不可能完全与某一级别的判断标准相一致，这就需要评估人员作出综合判断，确定风险级别。

（五）控制措施

选择恰当的控制措施以应对风险在现实中是一个复杂的问题。原因在于控制措施的执行及其效果受到多种因素的影响。因而，本文中的控制措施重在提供应对风险的角度，而非具体的方案。

那么，应对风险的角度如何确定呢？本文仍然从每个流程的控制目标入手。既然流程活动的目的在于达成每个具体的控制目标，那么控制措施只要能利于控制目标的实现，就是有效的风险应对措施。仍然以“战略规划风险”为例，其控制措施可从以下角度去确定：战略规划中充分考虑IT价值管理；建立IT战略规划和业务战略规划的双向交流和协调机制；评估IT解决方案及服务交付的现有能力；与有关的利益相关方共同编制战略规划；根据IT战略计划制定一整套组合的IT战术计划；考虑IT项目组合管理等。■

[本文系教育部2009年度人文社会科学研究项目(09YJC790033)和辽宁省高等学校重点实验室科研项目(WS2010002)的阶段性成果]

（作者单位：东北财经大学会计学院
青岛四方车辆研究所有限公司）

责任编辑 周愈博

● 词条

CCI指标

CCI指标(Commodity Channel Index)又叫顺势指标，是美国股市分析家唐纳德•蓝伯特(Donald Lambert)创造的一种重点研判股价偏离度的股市分析工具。CCI指标最早应用于期货市场的判断，后运用于股票市场的研判，并被广泛使用。与大多数单一利用股票的收盘价、开盘价、最高价或最低价而发明出的技术分析指标不同，CCI指标是根据统计学原理，引进价格与固定期间股价平均区间的偏离程度的概念，强调股价平均绝对偏差在股市技术分析中的重要性，是一种比较独特的技术分析指标。CCI指标专门衡量股价是否超出常态分布范围，属于超买超卖类指标的一种，但它与其他超买超卖型指标相比又有独特之处。像KDJ、WR%、CCI等大多数超买超卖型指标都有“0～100”的上下界限，因此比较适合研判一般常态行情，当面对那些短期内暴涨暴跌的价格走势时，就可能会发生指标钝化的现象。而CCI指标却是波动于正无穷大到负无穷大之间，因此不会出现指标钝化现象，这样就有利于投资者更好地研判行情，特别是那些短期内暴涨暴跌的非常态行情。CCI指标的应用法则如下：①CCI为正值时，视为多头市场；为负值时，视为空头市场。②常态行情时，CCI波动于100以内；强势行情，CCI会超出100。③CCI>100时，买进；直到CCI<100时，卖出。④CCI<100时，放空；直到CCI>-100时，回补。