IT外包风险、关键控制与审计策略

尤雪英(博士)

(上海海关学院经济与工商管理系 上海 201204)

【摘要】本文通过对IT外包风险的分析,探寻IT外包成功的关键控制,在借鉴国际内部审计师协会及世界最高审计组织有关IT审计框架的基础上,围绕IT外包的内部控制制度,就IT外包审计的目标、内容与方法展开论述,为完善我国IT外包审计提供对策建议。

【关键词】IT外包 风险 IT外包审计

一、引言

IT外包(ITO)是指组织将原来由自身提供的具有基础性、共性、非核心的IT业务和基于IT的业务流程剥离出来,全部或部分交由组织外部的专业服务提供商完成的经济活动。一个组织通过IT外包,可以充分利用外部专业化IT资源,实现一系列目标:降低IT运营成本,提高IT运行效率,改进IT 服务质量;更好应用IT前沿技术,增强对外部环境应变能力;培养IT专业人才,便利组织人事安排;增强组织核心竞争力,提高组织管理柔性等。根据互联网数据中心(IDC)统计,2012年,全球离岸服务外包市场规模为1 217.2亿美元,同比增长18.6%,其中,ITO占53.3%,BPO(业务流程外包)占21.9%,KPO(知识流程外包)占24.8%。ITO是服务外包产业中规模最大,发展最成熟的行业。

IT外包在给组织带来极大的便利与收益的同时,也隐含了巨大的风险。因此,本文将结合国际内部审计师协会(IIA)的Globe Technology Audit Guide 7"Information Technology Outsourcing"及世界最高审计组织(International Organization of Supreme Audit Institutions,简称INTOSAI)的IT审计工作小组发布的"Handbook on IT Audit",对IT外包的风险、IT外包的关键控制以及IT外包审计策略进行阐述。

二、IT外包业务的风险分析

1. 业务知识与业务流程的知识转移风险。IT外包是一种知识性行业,IT外包服务过程中发包方与服务商之间的知识转移是影响IT外包能否成功的关键因素。而知识转移所固有的复杂性、系统性、专用性、模糊性等特点,使得知识转移风险成为IT服务外包中的一项重要风险。

2. 知识产权保护风险。当组织与IT外包供应商处于不同国家时,因两国对知识产权保护的法律制度不同且保护水平不一,极易导致法律适用上的冲突。另外,IT外包是一种以信息技术为依托的服务模式,其专业性、技术性特点十分显著,涉及的知识产权问题繁多且复杂,因此,对知识产权的保护要求也远高于其他的服务外包行业。最后,由于应用程序是在组织外部开发的,组织很容易丧失业务流程的控制权,服务提供商在开发完毕后也往往会认为自己对有关的业务流程拥有知识产权。

3. 外包供应商无法按时交付风险。不完善的合同、有缺陷的供应商选择流程、不明确的里程碑管理或不利的市场条件,均可能导致供应商提供服务失败,从而致使供应商因时间紧迫或产品功能上的欠缺而无法按时交付。

4. 合同成本攀升风险。有三大主要因素会导致合同成本攀升。一是隐性成本。隐性成本发生在寻找供应商、签订合同,将企业内部的IT活动转交给供应商的移交成本,监控IT供应商完成合同规定的条款,与外包商讨价还价,以及就合同变更内容进行谈判的成本等。这些成本的发生有时会超过外包带来的好处,甚至完全抵消掉最初预计外包所能带来的成本节约。二是需求变更。由于所有的外包合同中都有基准和假设。如果实际的工作要求与合同中的需求有所不同,委托方将支付因需求变化而增加的成本,这已经成为IT组织所面临的最主要障碍。据大量的调查表明,绝大部分的IT外包项目将会在开发周期中因各种原因有大约10%~15%的变更。三是资产专用性与外包客户的专业程度,对成本上涨也有重大影响。但如果一味地降低成本,则可能影响资产专用性、客户端操作及所选择外包供应商的专业程度。

5. 关键人员变更风险。IT外包服务的快速增长创造了一个充满活力的劳动力市场。IT外包项目中关键人员往往会成为其他新的、更高知名度项目甚至是境外供应商高薪竞聘的人选,从而导致项目外包中关键人员的流失。

6. 境外供应商风险。聘用境外供应商所形成的风险将涉及对信息存储与转移的限制，数据可能会在组织并不知道的情况下被使用；因为要执行境外供应商所在国家的有关法律规定，安全与隐私标准可能并不能得到真正的遵循，而且基于不同司法管辖区的法律纠纷问题也不能完全避免。

三、IT外包的关键控制

1. 外包策略与政策。事实证明，造成**IT**外包失败的主要原因在于组织没有认真地选择哪些**IT**活动需要外包，哪些是应该自主研发的，以及组织没有制订适当的外包策略。

审计师应首先着眼于审查单位是否具有**IT**外包战略、政策与程序，**IT**外包策略是否符合组织目标。规模较大的组织往往会存在较大份额的**IT**外包业务。因此，具有一个成文的外包政策至关重要。一般而言，组织会把常规的**IT**运营、维护甚至桌面硬件平台外包出去，而把诸如人力资源管理、人事记录等功能保留在内部。因为这些都需要密切监测，如外包出去并不完全符合成本效益原则，并可能产生隐私与安全问题。规模较小的组织可能没有正式的外包政策，但应遵循高效、透明的招标程序。

2. 招标。招标是在记录系统要求和整理其他参考资料的基础上，生成招标文件包，发布招标信息，最终对供应商进行选择的过程。供应商遴选小组组长应由首席信息技术官担任，小组成员应包括组织内**IT**、财务、法律、人力资源部门及外包服务所涉及的部门。遴选过程应该透明和客观，并以相应的供应商遴选评价指标体系为依据，评价指标应能体现组织期望获得的系统或服务标准。

在招标过程中，事先进行详尽的尽职调查与风险评估非常重要，这不仅有利于对外包的潜在风险进行分析，对回报期、成本节约、供应链及客户影响等内容进行科学的事先评估，也能够避免对供应商的不当选择。

3. 服务级别协议（**SLA**）。**SLA**是组织与外包服务商之间具有法律约束力的协议，该协议建立起开发人员与客户之间理解与沟通的基础。**SLA**中应该明确定义服务供应商应当提供的服务以及这些服务的技术参数。

SLA中应包括以下内容：将由供应商提供服务的类型；组织和供应商之间的责任分配；将要测试的服务、测试周期、持续时间、地点、提交报告的期限（缺陷率、响应时间等）；实现新功能的时点、返工水平；由供应商提供的使用该项服务的文件内容及类型；运用外包服务的地点；备份频率以及数据恢复参数；奖励和处罚条款。

总之，所有被认为会对组织产生重要影响的关键项目都必须在**SLA**中予以反映。由于重要的技术参数都已记录在这些文件中，因此对**SLA**或其他文件（合同或正式协议）进行审查是**IT**审计师必须履行的职责。

4. 供应商（合同）管理。组织应定期跟踪项目的进展、服务质量，并在实际交付使用前对完工项目进行现场测试。此外，作为对外包供应商监测的一部分，组织还应该对外包供应商的内部质量控制与风险管理进行审计，以确保供应商能够按照合同规定的质量要求和时间计划做好各项工作。

审计师需要检阅在选择供应商前，组织是否已经在合同或**SLA**中以具体操作参数等方式明确对外包服务的各项要求，审计师还应该检查组织是否监控**IT**外包供应商去满足已经在**SLA**中的各项要求，并且当供应商不符合**SLA**中规定的参数时，组织是否已采取收取罚金或纠正措施等相应的行动。

5. 成本管控。在满足一定功能的情况下，当外包服务商提供相同服务的成本低于组织使用内部人力资源和基础设施的成本时，**IT**外包目标基本已经实现。虽然在外包中还会获得一些并不能直接估量的利益，如通过供应商的基础设施而迅速提高的服务水平等。但总而言之，从长期来看能否获得成本节约，仍然是进行继续外包或终止外包决策的重要依据。

6. 安全性。组织必须评估供应商是否在确保安全方面有足够丰富的经验。除了需引起高度关注的隐私问题外，误操作、敏感数据透露、非授权访问数据和应用程序以及灾难恢复计划都是可能发生的安全隐患。虽然这些问题很少会成为**IT**外包的重大障碍，但在文件中还是应该明确安全方面的要求。

四、IT外包审计的策略

IT外包审计是通过收集和评价客户**IT**外包管理活动和供应商**IT**外包服务活动，评价**IT**外包服务目标是否符合组织的目标，判断**IT**外包合同是否清晰定义并被遵守，对供应商的管理是否符合合同要求，数据安全是否得到保障，外包服务是否符合服务等级水平规定，以及**IT**外包在目标、功能、效益、成本方面的期望是否最终实现。

根据前述**IT**外包的委托方可能面临的风险以及外包成功的关键控制，围绕重要的控制措施，就如何开展有效的审计展开论述。

1. **IT**外包政策。审计目标：评价组织是否有一个明确、充分的**IT**外包政策。审计需要获知的信息：外包政策的文件、某一项外包的批准流程、全部外包项目的清单、部分外包项目的清单、某一项外包的成本效益分析、外包项目的批准文件等。

审计内容与方法：①审阅外包政策，并确保它已被批准，并逐条检查是否执行；②审阅外包的批准文件，确保得到高级管理人员批准；③审查相关文件，以评估该组织已经识别了针对不同的外包模式和不同地区外包服务提供商的风险；④审查相关文件，来验证该组织是否已知悉

在服务提供商被替换的不同可能性情况下的风险。

2. 招标。审计目标：评价组织是否有关于招标的政策，组织是否有明确的流程来识别和选择外包服务提供商。审计需要获知的信息：识别和选择服务提供商的流程、外包的项目连同服务供应商的清单、选择服务提供商的相关批准文件。

审计内容与方法：①文件审查，以确认该组织对招标制定有相应的政策；②审阅相关政策，以确保在主承包商将整个方案部分给了分包商的情况下，委托方拥有对分包商的数据请求权利；③审查文件，以评估关于招标的政策是否符合外包相关的法律；④审阅每一个承包或外包服务样本，判断遴选过程是否符合规定的政策；⑤审阅招标评价指标清单，了解组织是否有符合外包服务要求的指标清单。

3. 对供应商或承包商的监督。审计目标：评估组织是否对承包商或供应商进行了有效管理，当服务的性能或质量偏离基准时是否采取适当的行动。

审计需要获知的信息：服务级别协议、核准的进度表、界定外包产品或服务的技术参数、采取检查行为的文件/报告/会议纪要、偏差影响的评估报告、对偏离服务标准所采取行动的报告。

审计内容与方法：①审查文件，评估是否签署服务级别协议；②审查承包商所提供的检查报告，确认它们包含合同或服务级别协议中的重要因素；③审查监测报告，识别服务缺陷/偏差，评估由于缺陷/偏差产生的影响。

4. 数据权限。审计目标：评估组织是否在服务合同中对数据保护和访问权限进行明确规定，有没有一种机制来确保按照**SLA**的数据保护和安全要求确实被服务供应商采纳并实施。需要获知的信息：组织数据保护和访问权限的责任、对数据的定义（为了保护和访问权限）、与服务供应商的协议、由服务商提供的数据访问记录清单、第三方或内部审计报告的建议及相应的跟进行为、监控报告、由外包服务商披露给第三方/非相关方信息的清单。

审计内容与方法：①文件审查，确定数据保护的充分性、访问权限的要求、数据的定义符合规定；②审查与服务供应商签订的合同，检查数据保护及访问权限要求的履行情况；③审阅第三方或内部审计报告；④审阅监测报告、书信往来、事故处理报告，以评估组织采取的跟进行为；⑤审查非公开协议，以验证所有相关的信息均涵盖；⑥验证通过外包机构披露的信息是否得到授权。

5. 海外服务供应商。审计目标：确定组织是否了解将业务外包给海外机构可能产生的问题，是否对海外供应商承包的服务制定有相应的策略。需要获知的信息：涉及外包服务的法律或规定的清单、海外供应商所在国的能约束海外供应商的法律法规清单、东道国和服务提供商所在国家之间就促进外包业务所达成的双边协议、以往供应商在交付时间和质量方面的业绩报告、本土和海外服务供应商的成本效益分析。

审计内容与方法：①文件审查，以评估该组织已经明确了将业务外包给海外服务供应商的相关风险；②文件审查，以评估成本效益分析方法是否已解决将业务外包给海外服务供应商的风险；③文件审查，以评估已经对服务供应商进行了足够的背景调查。

6. 保留业务流程/知识的所有权。审计目标：评估业务流程的所有权是否已详细描述并记录在案，是否确保组织不会因外包而导致业务相关知识产权发生转移。需要获知的信息：对需要保留在内部的业务流程与关键技能的确认文件、关于业务流程的文件、关于组织外包服务的详细系统设计文件、对员工的培训清单（业务流程、系统设计、数据、应用软件方面）。

审计内容与方法：①文件审查，以评估组织已在合同中将业务流程、数据和应用软件的所有权保留在组织；②文件审查，评估有关数据、应用软件、系统设计方面的业务知识是否被记录并整理成文档，并进行定期更新；③文件审查，以评估目前与服务提供商之间并无任何关于系统和数据的所有权方面的事故或纠纷。

7. 成本控制与管理。审计目标：评估组织是否已确保涵盖外包合同整个生命周期的总成本是最经济的，组织已进行了必要的成本效益分析，组织也已明确是否有归属于组织的额外成本或不断增加的成本等内容。

需要获知的信息：必要的成本效益分析、外包服务的预测成本、基于成本要素的供应商遴选过程、有关遴选与审批流程的文档、服务供应商索取额外费用/不断增加费用的实例、对一些被不断要求增加费用/额外费用的监测报告、对服务供应商要求增加费用/额外费用采取行动的文件。

审计内容与方法：①文件审查，以评估外包中的所有费用已被组织识别，并经过了利益相关方的审查和批准；②文件审查，以评估所有成本均在合同中加以体现，不再会有任何未来费用等隐蔽费用；③查阅相关资料，以确定所有费用在组织承诺支付之前均经过了成本效益分析；④审查和比较合同成本的估计数与实际数；⑤审查服务供应商某项特定活动/功能的表现，评价某项特定活动/功能追加成本的必要性；⑥检查组织对服务供应商索取额外费用或追加成本的行为所采取的行动。

8. 服务级别协议。审计目标：评估组织是否已制定了详述其所有要求的服务级别。需要获知的信息：**SLA**或合同、由供应商实施的服务清单、组织与供应商的责任清单、对服务进行评价的相关数据指标（指标底限、评价周期、持续时间、地点和提交报告的期限）、有关服务的一些

社保资金联网审计系统构建初探

张永杰

（九江学院会计学院　江西九江　**332005**）

【摘要】面对社会保障信息化建设带来的新挑战与新任务，审计机关必须创新审计方式，构建与我国社保资金审计特征相适应的计算机联网审计系统。本文基于社保资金联网审计系统的研究，主要从系统构建概述、结构设计及其基本运作流程几方面进行分析。

【关键词】社保资金　联网审计　数据安全

一、社保资金联网审计系统构建概述

据统计，单纯审计我国每月养老保险参保个人的缴费记录和支付信息，全国社保信息系统产生的信息记录已超过**24**亿条。因此，开展社保资金联网审计已成为审计机关有效开展审计工作的现实选择。社保资金联网审计可以实现财务审计，还可以对复杂的数据进行审计。构建社保资金联网审计系统，首先需分析我国现行社保资金业务经办流程及审计流程，明确具体构建目标。

1. 社保资金业务经办流程。我国社保资金业务经办的基本流程（如图**1**所示）包括社保资金的征收、管理和发放等主要环节，具体涉及社保资金的登记管理、缴费核定、资金征缴、资金核算、账户记录、待遇核准、资金测算与资金支付等流程。

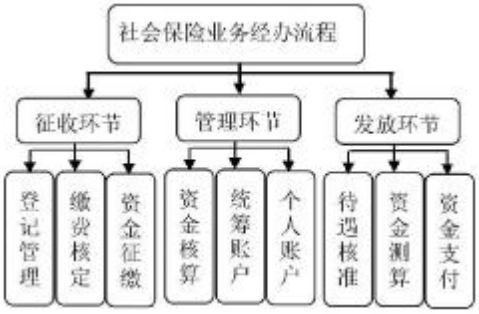

图 1　社保资金业务经办流程

其中，养老保险资金、医疗保险资金和失业保险资金由用人单位和劳动者个人同时缴费，养老保险、医疗保险都涉及个人账户；工伤保险资金和生育保险资金由用人

指标（如缺陷率、回复时间、帮助操作人员时间等）。

审计内容与方法：①文件审查，以评估所有的用户需求都被转化为**SLA**中的要求；②文件审查，以评估该组织和服务提供者的角色和职责都被明确地界定；③文件审查，以评估关于服务等级的参数已经明确，并包括在**SLA**中；④文件审查，以确认服务水平监测机制已建立并得到组织和服务供应商的认可；⑤审查供应商的报告，以确认在**SLA**中的参数出现在报告中，并由组织内部相关人士审阅；⑥检查组织对服务水平协议偏差所采取的行为。

9. 安全。审计目标：评估有关外包的安全要求是否得到解决和遵守。需要获知的信息：组织的安全政策、**SLA**、在外包服务地的访问控制日志（关于数据文件、应用软件以及硬件）、对于备份网站和灾难恢复站点的安全计划、关于安全问题的监测报告、就安全问题组织与服务供应商之间的通信往来。

审计内容与方法：①文件审查，以评估安全要求已被组织明确识别并写入外包合同或**SLA**；②验证组织是否有关于数据文件、应用软件的目录清单；③验证组织已监控/意识到数据文件、应用软件和硬件的状态在外包机构进行的备份和数据恢复过程中均被保留下来；④验证组织是否已确保外包机构对数据、应用软件和硬件的任何改变均需得到授权；⑤验证组织是否能够通过查阅访问日志（物理和逻辑）以确保在外包地点对数据、应用软件和硬件的访问控制；⑥验证组织是否能收到定期监测报告并依据监测报告中的信息采取行动。

【注】本文系海关总署科技司课题“海关信息应用开发模式研究”（编号：**2312116**）的阶段性研究成果。

主要参考文献

Chen Yongqiang, Yang Huansong, Hong Libin.Analysis and thinking of failed Japanese ITO cases in China.International Journal of Networking & Virtual Organizations, 2012;10