持续审计:应用概况与实施步骤

王佳欢

(南京审计学院审计与会计学院 南京 211815)

【摘要】持续审计是在借助先进信息技术的前提下对传统审计模式进行的一次革新,是审计工作在当前科学技术条件下的延伸。本文介绍了持续审计的理论基础,分析了其应用概况,重点阐述了企业实施持续审计的条件与关键步骤,并剖析了潜在的风险及其预防措施,以期能够促使持续审计在我国企业顺利有效地开展。

【关键词】持续审计 风险领域 成本收益

电子商务的瞬间性、信息报告的及时性以及针对内部控制与欺诈相关法案的颁布,使得受到了会计周期的制约的传统审计方法与模式受到了挑战,难以满足现行的经济环境对审计的需求。而持续审计具有及时性、全面性与程序自动执行的优点,有利于提高内部控制的有效性,促进信息报告的及时提供,减少企业遵循**SOX**法案的成本,提高审计的质量与效益,是审计领域的发展必然趋势之一。因而如何促使企业有效开展持续审计,有着重大的现实意义。

一、持续审计的理论基础与定义

委托代理理论、信息不对称理论、事项会计理论与全面质量管理理论是持续审计产生的理论基础,它们对审计需求的变化促进了审计模式的变革。

由于社会需要的层次与水平不断提高与发展,委托代理的内容也呈现出不断扩展的趋势,这也是审计模式不断分化、发展创新的内在根源。信息不对称理论认为对会计信息的审计有利于缓解信息内外部使用者的信息不对称,提供审计的成本与消除信息不对称带来的收益之间对比关系的变化,推动了审计模式的演进,促进了持续审计的出现。事项会计理论主张按照具体的经济事项来报告企业的经济活动,促进了网络实时财务报告模式的兴起,对及时有效的审计模式产生了需求。全面质量管理的实质是以顾客满意、附加价值和持续改善为核心的一种全面经营管理理念。审计要加强自身的质量管理,必须对传统审计模式进行改进,全面跟踪企业的经营过程。

持续审计的定义一直在不断地发展。**1999**年,**CICA**与**AICPA**联合发布了一份《持续审计》的研究报告,由此提出了"持续审计"的思想,并将持续审计定义为"一种由独立的审计人员使用的,在一系列的审计报告的基础上,为一个企业管理当局承担责任的项目提供书面保证的技术,这些审计报告发布时间与事件发生时间是同步的或者紧随其后的",此定义体现了持续审计的及时性。**2005**年**IIA**发布的《全球技术审计指南》将持续审计定义为"一种利用技术自动执行控制和风险评估的方法,是审计策略从传统的交易样本的周期性复核向对所有交易持续测试的转变",此定义体现了持续审计程序自动执行与全面测试的特点。

尽管各个定义对持续审计的内涵理解各不相同,但是与传统审计模式相比,持续审计基于信息技术,审计范围广泛、审计时间及审计报告具有及时性且强调程序自动执行等特点。

二、我国持续审计应用受到的阻碍

持续审计在西方发达国家应用较早而且发展迅速。在全球范围内,应用持续审计的企业涉及的行业包括共同基金、银行业、零售业、医疗保健与制造业等。虽然我国企业已经普遍采用**ERP**等信息系统,证券公司还建立了实时交易监控系统为核心的中央监控系统,工商银行开始尝试对信贷业务进行持续审计。但是在我国大部分的企业中,持续审计没有真正的开展起来。

1. 成本效益方面。持续审计过程开发和实施成本较高,**IT**环境配置、相关软硬件购置,程序的运行、更新与维护,对原有审计人员进行培训,这些都将产生高昂的费用。企业实施持续审计带来的收益主要包括能够有效地评估内部控制、紧跟关键控制、及时获取相关事件、减少审计资源耗费与提高审计效益等。显然,这些投资回报很难量化。当投资成本巨大,回报无法直接计量时,投资者在制定决策时容易顾虑重重,犹豫不决。

2. 持续审计技术应用方面。审计人员实施的持续审计与管理员实施的持续监测等系统会对相同的指标进行监控,这会引起信息超载和警报泛滥的问题,同时也会影

响系统的运行效率。持续审计技术功能仅限于数据的持续审计，对内部控制评价与风险评估仍然离不开审计人员的专业技能。

3. 审计人员的能力与心理方面。持续审计带来的审计频率、审计报告等变化对审计人员的技能提出更高的要求。截至目前，国内对持续审计的研究很少涉及持续审计具体应用，这为审计人员提高自身技能造成了一定的困难。连续审计要求运用自动化程序，这会引起审计人员工作的稳定性与工作地位的担忧，阻碍审计人员接受持续审计。

三、实施持续审计的条件

根据**2005**年**IIA**发布的全球技术指南，实施持续审计的条件主要有各参与方的网络服务器相互连接、可靠的系统、高度自动化的程序提供审计证据、审计人员具备良好的能力等。

1. 持续审计要求参与方的网络服务器能实时、准确和安全地相互连接。审计人员通过网络服务器连接企业的信息系统以获取所需数据，连接管理层及其他部门，将审计发现传送给管理层和相关部门，连接信息使用者以满足他们对及时地发布审计报告的使用需求。

2. 实施持续审计需要可靠的系统。系统可靠性的原则包括完整性、安全性、可用性以及可维护性。可靠的系统是完整准确地获取所需信息，防止来自企业内部或外部的非法入侵，向信息使用者提供审计报告以及在必要的情况下更改维护系统的前提。

3. 高度自动化的程序。企业需要设置高度自动化的程序，自动地提取数据并将数据与原先设置的标准进行比对以发现异常，这是提高效率，降低成本的关键所在。

4. 审计人员具备良好的能力。持续审计是基于信息技术的审计，但是连续审计不可能完全自动化，审计人员必须能够分析出现异常情况的交易以及分析其他数据，发现问题。同时，也需要对结果进行分析，发布恰当及时的审计报告。

四、有效开展持续审计的步骤

基于持续审计程序与传统审计程序的共同点和差异，**IIA** 研究报告对持续审计程序进行了较为系统和完整的论述，关键的审计程序包括以下五个方面。

1. 确定持续审计目标。持续审计系统建设前期投入较大，因而在实施之前，明确持续审计的短期目标与中长期目标，有利于持续审计在企业的稳步开展。

第一，应考虑实施持续审计的效果性。若选择长时间内才体现其效果，则会降低对持续审计的支持。持续审计的目标应该具体明确，如果试图对一个跨国公司的全部财务资料进行持续审计，难度很大。相反，仅对日常生产、运输、销售及其他容易计量和较少运用职业判断的事件进行持续审计，则要容易得多。

第二，应重点关注高风险领域。内部审计人员从风险集中的领域去实施持续审计，因为潜在的风险一旦发生将会使企业发生严重损失。例如在医疗保健行业，个人隐私的保护成为民众关注的热点之一，因而应当在电子医疗的记录上实施监控与审计。选择重点审计的组织领域应该被整合为内部审计年度计划与该公司的风险管理计划活动的一部分。如果公司已经制定了风险管理框架，应参考风险管理框架，同时也要关注以前年度对公司实施重点审计的领域。

第三，应考虑公司管理层的支持力度。要将准备工作，尤其是有关数据的存取需求，以及何时、何种方式向公司管理层报告审计结果。否则，持续审计活动的合理性可能就会遭到质疑。

2. 进入被审计单位信息系统，获取数据信息并进行数据预处理。在真正开展持续审计之前，需要将企业内部各部门不同的信息系统进行整合，以便数据的传输与信息的发送。实施持续审计需要审计人员有权直接访问企业信息系统，然而对审计人员信任度的缺乏和对组织信息系统安全性的考虑，会阻止管理层接受持续审计。西门子公司在实施持续审计过程中，全面检查**ERP**审计流程，并尽可能提高自动化程度。公司选出一些耗时长、成本高的审计活动，将其自动化，比如与流程的控制人员访谈，询问是否已经实施必要的控制措施等。同时，西门子使用了电子软件检查采购付款循环交易和差旅费管理。

企业的信息系统之间应该明确分工，减少重复任务安排。应正确的区别持续审计与持续监控，两者之间具有一定的相似性，都是对内部控制中交易和系统活动进行自动化测试。将持续审计与持续监控各安其职，在保证审计人员独立性的基础上，可以增加系统相互之间的协调性，同时可以最大程度的发挥自身的价值，减少内部控制上的重复与公司系统的负担，相应地减少在人力财力上的不必要浪费。

3. 持续控制评估和持续风险评估。持续控制评估通过预先设计的控制测试来对交易数据进行独立的分析，不仅包括对例外情况的简单识别，也包括更加复杂的内部控制评估。

对例外与异常的识别只是审计过程中的一步。审计人员还需要审查所拥有的资料来评估审计中发现的问题。认真审视结果以便发现异常中存在的错报，同时根据特定的环境微调筛选的规则，保留下值得注意的高风险问题。内部审计员的工作不是去盯住每一笔交易，也不是盯住每一件异常的事件，而是在这个流程中加入透明度指标，并审视在整个时间段出现的控制问题是什么性质。在设定连续的审计程序时，要设置合理数据的范围以及

故障阈值,范围的设定应该随着环境变化而相应的调整。例外事项可能是产生的假象,显示的例外事项实际上是正常事项,这就需要调整测试所用的判断标准。

持续风险评估是识别被评估的实体以及其所面临的风险。审计人员必须了解企业内部与外部环境,分析潜在的风险领域,了解企业的风险偏好,并对识别的风险进行排序。审计人员在持续风险评估时可以采用风险指标持续评估法,风险指标是对与活动或流程相关的控制有效性或潜在威胁的量化,持续风险评估可以对整个控制领域的风险状况进行定期的、结构化的评估。

审计人员需要评估控制环境。如果公司已经指定了风险管理框架,审计人员应当检查控制框架与风险管理框架所涉及的范围。如果管理层建立并拥有运营良好的流程用以评估控制与风险,审计人员可以更多地依赖公司提供的控制。但是,如果公司流程不充分,审计人员需要持续地实施更加详细的控制和风险评估。

4. 确定持续审计的频率和时间。持续审计频率的确定主要取决于三个因素:一是企业的系统或程序的风险水平,二是管理层实施监控的充分性,三是实施持续审计的成本。当企业内部控制为低风险水平时,可以减少持续审计的频率。缩短持续审计的时间,反之,则提高持续审计的频率,增加持续审计的时间。同样,管理层监控的充分性与持续审计的频率成反比。持续审计的成本增加,会相应地减少实施持续审计的频率。

为了最小化持续审计的运营成本,**Pathank et al**(**2005**)运用随机过程分析了一个大型数据库进行持续审计,采用计次与计期的战略模型。计次审计是在**n**次商业交易之后才对数据库的错误和其他不合规的情况进行审计,计期审计是审计人员在每一个较为固定的短时间**p**后对数据库进行审计。持续审计成本分析的关键就是对最佳次数**n**和最佳的时间间隔**p**的选择。如果**n**或者**p**过大,就不能有效地查找数据,但如果**n**或者**p**过小,持续审计的成本就要增加。计次审计和计期审计都对错误有个可接受的水平,而且审计及时性与准确性之间存在着相互替代关系,对准确性的要求过高,就会增加成本的需求,如果对及时性的要求过大,就会增加审计错误的数量。

在假设交易数据到达数据库是满足**Poisson**分布的前提下,得出最佳次数**n**为:

$$n=\sqrt{\frac{2r(1-rE(t))A}{a}}$$

最佳的时间间隔**p**为:

$$p=\sqrt{\frac{2A(1-rE(t))}{ar}}$$

其中,**r**为单位时间内到达的交易次数,**E**(**t**)为审计一项交易需要的时间,**A**为每次审计的固定成本,**a**是审计滞后的成本。

5. 出具审计报告及跟踪审计建议。持续审计报告发布的形式和频率与传统的内部审计报告有所不同。在形式上,持续审计的审计报告形式更加多样化,比如通过网络发布。关于频率,持续审计的审计报告相对于传统审计更加频繁,更加及时。

审计人员需要对审计报告中的事项按重要性排序,考虑进一步应对的程序,并对其采取措施的同时根据重要程度考虑与审计委员会和管理层沟通。审计人员还要跟踪审计建议,以确定管理层是否已经执行,以及审计建议是否被采纳等。由于审计测试需要不断改进,产生例外事项的报告及其后续行动突出哪些异常参数需要修正,审计计划就变成了一个反复修订的过程。

五、实施持续审计的潜在风险及预防措施

企业实施持续审计却蕴含着潜在的风险,主要有信息存储风险与数据传输风险等。主要是指从互联网对企业的数据库和服务器进行入侵,破坏系统的数据文件,干扰硬件的正常运行,进而对持续审计造成影响。非授权访问和冒充合法用户都是这类风险的常见形式,这类攻击可能来自企业内部,也可能来自企业外部。同时,大量的企业信息在审计部门,企业其他部门需要时,在传递的过程中,数据信息不可避免地受到外界的影响,可能会被非法截获与篡改。

因此,应该制定全面的信息安全解决方案,有针对性地抵御各种威胁。企业可以通过部署统一的网络防病毒系统、安全可靠的防火墙以及入侵检测系统等来维护信息的存储安全。同时,可以通过应用数据加密技术与应用数据库安全技术防范数据传输风险。

主要参考文献

1. 毕秀玲.持续审计基本问题研究.审计研究,**2008**;**4**

2. 惠迎.持续审计及其审计程序设计——以应收账款审计为例.中国管理信息化,**2010**;**11**

3. 张文秀,刘雷.持续审计.大连:东北财经大学出版社,**2012**

4. 张栋.持续审计的若干问题探析.经济视角(中旬),**2011**;**11**

5. 谢筠.连续审计的开展及应用.中国管理信息化,**2008**;**3**

6. 安宁.内部持续审计:可行性分析与应用框架.财会月刊,**2011**;**21**

7. 郝东洋.连续审计在我国的应用.企业家天地,**2008**;**10**

8. 陈颢.连续审计背景下的经济可行性研究.中国商贸,**2013**;**14**