XBRL环境下内部控制审计框架研究

戴 利

（湖南大学工商管理学院 长沙 410082）

【摘要】XBRL的研究与应用不断发展和深入，将该技术应用到内部控制审计领域成为必然趋势，本文探讨了在XBRL内部控制评价报告和传统内部控制评价报告并存及XBRL内部控制评价报告替代传统内部控制评价报告环境下的内部控制审计框架。

【关键词】XBRL 内部控制 审计框架

一、研究背景

为了促进企业建立、实施和评价内部控制，财政部会同证监会、审计署、银监会和保监会于2010年制定并发布了《企业内部控制规范》，自2012年1月1日起在上海证券交易所和深圳证券交易所主板上市公司施行，并要求披露年度自我评价报告，同时还要聘请会计师事务所对财务报告内部控制有效性进行审计并出具审计报告。随着XBRL的不断发展和深入，XBRL技术应用于内部控制审计也成为一个必然趋势。

以往关于XBRL的研究主要集中于：XBRL分类标准，以及XBRL对财务报告审计的影响和XBRL财务报告审计方法。本文在以往研究的基础上进行延伸，探讨XBRL环境下内部控制审计框架，促进XBRL技术的广泛应用和内部控制审计的高效合规开展。

二、XBRL内部控制评价报告和传统内部控制评价报告并存环境下的内部控制审计框架研究

财政部会同证监会、审计署、银监会、保监会制定的《企业内部控制审计指引》规定，“建立健全和有效实施内部控制，评价内部控制的有效性是企业董事会的责任”，“对内部控制的有效性发表审计意见是注册会计师的责任”。因此，财务报告内部控制审计是基于责任方认定的鉴证业务。即注册会计师对管理层发布的内部控制评价报告中关于内部控制有效性的认定进行鉴证，对内部控制有效性发表审计意见。

目前XBRL的应用主要集中于财务报告方面。XBRL在内部控制审计方面的发展轨迹预计和在财务报告中的应用相似。虽然XBRL技术自1998年提出，至今已十几年，但目前在财务报告中的应用仍处于XBRL财务报告与传统财务报告并存阶段，只有经过并存阶段的不断探索最后才能实现XBRL财务报告对传统财务报告的替代。将XBRL引进内部控制领域，也必然会经过XBRL内部控制评价报告（以下简称“XBRL报告”）与传统纸质内部控制评价报告（以下简称“传统报告”）并存阶段和XBRL报告替代传统报告两个阶段。

下文将对XBRL报告与传统报告并存环境下的内部控制审计框架进行研究。《企业内部控制审计指引》特别强调了风险导向审计思想，要求注册会计师按照风险导向审计模式，采用自上而下的方法开展审计工作，并将其作为识别风险、选择拟测试控制的基本思路，因此本文拟构建的内部控制审计框架按照这一要求构建，对审计目标、风险评估和风险应对分别进行阐述。

1. 审计目标。内部控制审计的目标是对内部控制有效性发表审计意见，对内部控制评价报告中关于内部控制有效性的结论进行确认。在XBRL报告和传统报告并存的环境下，传统报告已经经过外部审计师的审计，因而此时内部控制审计具体目标主要是确认XBRL报告完全反映传统报告，为实现这一目标的相关认定及认定对应的具体目标在随后的风险评估部分进行详细介绍。

2. 风险评估。在两种报告并存环境下，重大错报风险主要存在于将传统报告映射到XBRL报告过程中，可以分为认定层次重大错报风险和报告层次重大错报风险。高锦萍（2011）认为在将传统报告映射到XBRL报告过程中的管理层认定主要有三个层次：关于XBRL 财务报告中商业事实的认定，关于XBRL 财务报告中元素映射（标记）的认定，关于XBRL 财务报告中元素拓展的认定。林琳、潘琰（2011）重新定义的XBRL环境下的管理层认定体系由与XBRL实例文档数据相关的认定、与XBRL 实例文档元数据相关的认定以及与XBRL分类标准相关的认定构成。聂萍、汤洋和杜碧莹（2013）则基于XBRL财务报告元素的角度构建了元素标记相关的管理层认定体

系。本文在以上文献的基础上构建传统报告向XBRL报告映射过程中的管理层认定体系。

由以上文献可知，在将传统报告映射到XBRL报告中主要是实现商业事实的完全真实反映，在实现这一目标过程中的认定及认定对应的具体目标主要有：①完整性。完整性认定对应的具体审计目标是XBRL报告将已审传统报告中的所有相关商业事实包括进来，如果一个已审报告中包含的对内部控制缺陷评价在XBRL报告中没有体现，则构成使XBRL报告与已审传统报告不一致的重大错报风险。②存在性。XBRL报告中披露的商业事实是确实存在的、已发生的且与被审计单位有关，即已审传统报告中没有披露的商业事实在XBRL报告中也不应被标记。如果存在XBRL报告中披露而已审传统报告未披露的商业事实，则也会构成XBRL报告与已审传统报告不符的存在性认定重大错报风险。③准确性。XBRL 报告中关于各个控制的缺陷的描述应与传统报告一致。如果存在对内部控制的评价不一致的地方，则构成准确性认定方面的重大错报。

报告层次重大错报风险是指与报告整体广泛相关、会影响多项认定的风险，在两种报告并存环境下，报告层次重大错报风险是指将传统报告映射到XBRL报告过程中不符合XBRL技术规范以及语法规则的风险。由于此类风险主要由将传统报告转化为XBRL报告的软件的有效性决定，而映射过程中所使用的软件存在瑕疵则导致整个XBRL报告不符合规范，这类风险并不是只对某项认定有影响，而是会影响到多项认定。因而，此类风险归为报告层次重大错报风险。

3. 风险应对。对于认定层次的重大错报风险，审计人员采取的风险应对措施主要是实质性测试。对于完整性认定，可以采取审计程序中的检查法，审计人员可以将已审传统报告作为起点，追踪至XBRL报告，即采用顺查法检查已审传统报告中的所有商业事实均被标记。对于存在性认定，审计人员可以 XBRL报告为起点，追踪至已审传统报告，采用逆查法检查XBRL报告标记的商业事实是不是传统报告中所披露的。准确性认定的审计程序也采用检查的方式，通过顺查和逆查核对XBRL报告和传统报告关于内部控制有效性的评价是否一致。

对于报告层次重大错报风险，审计人员采取的应对措施为控制测试。主要是采用对软件进行校验的方式，检测软件的功能是否符合要求。可以通过对生成的实例文档进行校验的方式来测试完成转换的软件是否合规，主要检查生成的实例文档是否符合XML语言规范、是否符合技术规范以及分类标准要求。

两种报告并存环境下的XBRL内部控制审计框架可以用图1表示：

图 1 两种报告并存环境下的XBRL内部控制审计框架

三、XBRL报告替代传统报告环境下的内部控制审计框架研究

在替代环境下，XBRL内部控制审计框架也可包括内部控制审计目标、风险评估和风险应对。在XBRL系统条件下，鉴证的内容应包括XBRL的开发与设计、会计数据库文件和内部控制的审计以及数据输入输出的审计，同时还必须对XBRL系统的内部控制制度、XBRL系统的应用程序、存储在磁性介质上的数据文件、系统开发以及对XBRL系统硬件本身的可靠程度即整个企业信息系统的安全可靠性进行审计。

本文拟构建的替代环境下内部控制审计框架基于COBIT（信息及相关技术的控制目标）模型。COBIT由信息系统审计与控制协会在1996年公布。这是一个在国际上公认的、权威的安全与信息技术管理和控制的标准，目前已经更新至5.0版。它在商业风险、控制需要和技术问题之间架起了一座桥梁，以满足管理的多方面需要。该标准体系已在世界一百多个国家的重要组织与企业中运用，指导这些组织有效利用信息资源，有效地管理与信息相关的风险。COBIT将IT过程、IT资源与企业的策略和目标（准则）联系起来，形成一个三维的体系结构。本文替代环境下的内部控制审计主要基于COBIT 模型，以IT资源为审计对象，关注IT资源不符合IT准则的要求的风险，并提出相应的风险应对策略。

1. 审计目标。当XBRL技术在企业得到普遍应用、企业财务信息系统均开发出相应的分类标准时，XBRL报告就会替代传统报告，内部控制评价报告就单独以XBRL形式披露。替代环境下，内部控制审计目标就是传统的内部控制审计目标，即对内部控制有效性发表审计意见，合理保证内部控制合法、有效、充分和适宜。此时由于各个财务系统都应用XBRL技术，企业的数据能够实现多方共享，不再需要先生成纸质报告而后再转化为XBRL形式，因此在替代环境下，XBRL报告完全反映传统报告这一具体目标不再存在。

在替代环境下，本文内部控制审计重点关注与XBRL技术相关的内部控制。由于所有财务数据的生成都是依托于信息系统，利用XBRL技术进行处理，因而替代环境下内部控制审计重点是信息系统审计。在替代环境下，内部控制审计可以类似于信息系统审计而分为一般控制审计和应用控制审计，一般控制审计面向系统，应用控制审计面向数据。

2. 风险评估。在替代环境下，内部控制审计风险是指审计师对内部控制发表不恰当意见的风险。在替代环境下，本文的内部控制审计以COBIT模型中的IT资源为审计对象，主要包括技术、设备、人员、应用系统和数据。按照前文的面向系统的一般控制审计和面向数据的应用控制审计的划分，将IT资源中的技术、设备和人员划分到面向系统的一般控制审计，将应用系统和数据划分到面向数据的应用控制审计，然后探讨在替代环境下内部控制过程中各审计对象不符合IT准则的风险。IT准则主要包括有效性、效率性、保密性、可用性、符合性和可靠性。

（1）替代环境下，技术包括硬件、操作系统、数据库管理系统、网络和多媒体等相关技术，技术上的风险主要是不符合有效性准则和效率性准则的风险。技术上的有效性风险是指企业未掌握XBRL技术，不能将XBRL技术应用于企业的财务信息系统和发挥XBRL技术的优势。而技术上的效率性是指IT管理层应重点关注系统软件参数的设置和维护，系统软件参数由适当的IT人员选择正确的参数，以确保存储在系统中的XBRL数据和XBRL程序的完整，确保所安装系统软件的设置不会危及已经存储在系统中的数据和应用程序的安全。技术上的效率性风险则是企业技术为达到技术效率性的要求的可能性。

（2）设备是指支持XBRL应用于信息系统的所有资源，设备上的风险主要是指有效性风险。设备有效性风险是指企业信息系统硬件不能满足软件以及技术不断发展的要求，或者硬件设备处于一个不安全的物理环境，容易产生盗窃或故意破坏所造成的损失或毁坏，而IT管理层未能采取足够的措施抵御环境因素（如火灾、灰尘、动力、过热或过湿）的破坏，未能对硬件进行日常和定期的硬件维护，以减少性能故障的发生频率和影响。

（3）人员主要是指员工技能、意识以及计划、组织、交付、支持和监控信息系统及服务的能力，人员的风险主要有有效性风险、效率性风险和合规性风险。

人员有效性是指机构中所有人员都理解其相关信息系统中的角色和责任，并有能力和资源能够胜任其职责，并且企业各角色的设置考虑了适当的职责分离，没有人能够控制一个交易或事件的所有关键环节。人员效率性是指机构岗位和职责的划分保持高效率，防止机构重叠、人员冗余或缺失，管理层能确保知识和技能需求被不断地评估，并且要保证机构能够获得一个达到机构目标所需要的具备相匹配技能的工作队伍。人员合规性是指人员遵从法律法规以及合同承诺的独立保证。若人员不能达到以上要求，则存在以上方面的风险。

（4）应用系统是指手工及计算机程序的总和，应用系统的风险主要是保密性风险、可用性风险、有效性风险、效率性风险及完整性风险。

保密性是指保护敏感信息免于暴露给未经授权的人，应用系统的保密性是指应用逻辑访问和IT计算资源的使用应由适当的识别、鉴别、授权的机制所限制，用访问规则连接用户和资源，这样的机制应能防止未经授权的人员、电话拨号连接和其他系统（网络）入口访问计算机资源，并使授权用户多个登录的要求最小化。应用系统可用性是指业务和IT管理层应确保建立一个跨越全机构的程序，避免信息系统和技术遭受计算机病毒的侵害，以保持应用系统使用的连续性。应用系统有效性是指管理层应采用开发、获取、实施和维护计算机化信息系统和相关技术过程的系统开发生命周期方法，挑选的系统开发生命周期方法应适合被开发、获取、实施和维护的系统，应用系统在投入使用前应进行检查测试。应用系统的效率性是指无论系统采用购置还是内部开发的方式，都应进行成本效益分析，符合成本效益原则，而且要对软件进行适当的参数设置，以防参数设置不当导致软件运行效率低下。应用系统完整性是指对于来自第三方供应商带有用户许可证的XBRL软件，管理层应要求供应商通过适当的程序来验证、保护和维持该软件的完整性，要防止所有涉及硬件和软件安全的损害，以维持它们的完整性。

（5）数据是指信息系统处理的财务数据，在替代环境下，主要指XBRL实例文档。数据的风险主要包括XBRL实例文档的有效性风险、可靠性风险以及保密性风险。

XBRL实例文档有效性风险是指实例文档是否满足XBRL技术规范、分类标准要求的风险。XBRL实例文档可靠性风险是指实例文档中所载信息内容是否真实，机构应建立合适的程序，确保数据只能由授权人员输入，提交、通过、授权和数据录入功能之间应适当职责分离，管

理层应确保对XBRL实例文档在传输和传递过程中的充分保护，防止未经授权的访问、修改和寄错。XBRL实例文档保密性风险是指实例文档能否安全披露，不被黑客侵袭，未经授权不会被更改，管理层应建立安全程序如口令、保护终端安全措施、数据加密措施、防火墙控制、病毒保护等，防止企业的敏感数据被窃取，当计算机、磁盘、其他设备或介质废弃或传递给其他人使用时，要防止对其中的敏感信息和软件的访问，保证标记着删除或废弃的数据不能由内部或第三方恢复出来。

3. 风险应对。在替代环境下，对于内部控制审计上述风险的主要应对措施是采取控制测试。对于技术上的有效性风险，可以通过询问企业相关工作人员对于XBRL技术的了解、观察工作人员利用XBRL技术进行业务处理的过程、检查企业生成的XBRL相关文件是否合规来检查；技术上的效率性风险主要通过对软件进行测试来检查。

设备的有效性风险可以通过检查企业对设备的管理政策及具体的管理方式来检查。

人员的有效性风险可以通过检查相关人员的任职资格，询问其对XBRL技术的了解和掌握程度来检测；人员的效率性风险则通过查阅企业规章对岗位的设置是否合规来检测；人员的合规性风险也可以通过询问相关工作人员对业务处理过程的理解、检查相关业务处理结果来检测。

应用系统的保密性风险、可用性风险、有效性风险、效率性风险及完整性风险都需要采用对应用系统进行测试的方式检查，看应用系统是否满足保密性、可用性、有效性、效率性和完整性。

对于XBRL实例文档的有效性风险，主要通过检查XBRL实例文档有效性来检测生成实例文档的软件是否存在内部控制风险；对于XBRL实例文档的可靠性风险，主要通过检查XBRL实例文档生成流程中岗位分离、业务处理相关人员的独立性和胜任能力来检测；对XBRL实例文档保密性风险，主要通过检查实例文档处理以及保存过程中对接触实例文档的授权是否严格和科学来检测。替代环境下内部控制审计框架见图2。

图 2 替代环境下内部控制审计框架

四、结论

本文探讨了XBRL环境下内部控制审计框架，尝试构建了XBRL报告与传统报告并存环境下和替代环境下的内部控制审计框架。内部控制审计框架由审计目标、风险评估和风险应对构成。

在两种环境下，内部控制审计目标都是对内部控制有效性发表审计意见，但两种报告并存环境下的具体审计目标为对传统报告向XBRL报告映射过程的准确无误发表审计意见。并存环境下的审计风险主要关注映射过程中可能出现的风险并采取实质性程序和控制测试进行风险应对；替代环境下的风险评估主要基于COBIT模型，评价IT资源可能面临的不能满足IT准则的风险，然后采取控制测试的风险应对方法。

本文初步探讨了XBRL技术在内部控制审计中的应用，为XBRL环境下内部控制审计模型构建提供一个框架，具体深入研究还有待进一步展开讨论。

主要参考文献

1. 张天西.网络财务报告：XBRL标准的理论基础研究.会计研究，2006；9

2. 高锦萍.XBRL财务报告审计模型及实现机制：一种框架研究.审计研究，2011；3

3. 林琳，潘琰.XBRL鉴证业务理论基础构建.当代财经，2011；8

4. 许渊，李建义.XBRL的应用及其对审计的影响.财会月刊，2005；10