论信息化内部控制审计与信息系统审计

厦门大学管理学院　魏森淼　庄明来

《内部控制审计指引》以及《内部控制审计指引实施意见》的发布与实施，使我国的审计体系更加趋于完善。众多理论研究者从不同角度探讨了内部控制审计与财务报告审计的关系及其整合问题，但对信息化内部控制审计与信息系统审计之间关系的探讨甚少。信息系统审计在国外方兴未艾，在我国却处于起步阶段。随着信息技术应用的不断深入，成功地开展信息系统审计，是我国审计走向世界的必由之路。内部控制审计和信息系统审计共同构筑了财务报告信息质量保证体系，信息化环境又使二者的界限变得模糊，从而不得不思考：在信息化环境下，仅仅实现财务报告审计与内部控制审计的整合是否合适？是否应对财务报告审计、内部控制审计和信息系统审计进行全面整合？为此，厘清信息化内部控制审计与信息系统审计的联系与区别显得尤为重要。

一、信息化内部控制审计与信息系统审计的相关规范

国内外相关规范中的一系列规定表明，现代内部控制审计必须充分重视信息技术的应用。信息技术在财务报告内部控制领域的应用，主要的表现形式就是信息系统，特别是会计信息系统的建立。信息化内部控制审计关注会计信息系统的内部控制有效性问题，而这个问题也是信息系统审计关注的重要内容之一。而国内外一系列信息系统审计规范的陆续发布，又使信息系统审计成为人们关注的热点。信息系统本身就包含了信息技术的应用，信息技术的深入应用又对信息系统的内部控制产生重大影响。而信息系统，特别是会计信息系统的内部控制，同样是信息系统审计中重要的一环。

（一）信息化内部控制审计　会计信息质量不仅取决于财务报告本身，更取决于对财务报告产生过程的有效控制。内部控制是防范企业财务报告错误和舞弊行为，保证企业财务报告真实、完整的内在机制。而内部控制审计的目的就是要评价内部控制的有效性。信息技术应用的不断深入使经营管理越来越依赖于利用信息技术建立起来的信息系统。理论界也密切注意着信息化环境下企业内部控制制度的变化，许多学者纷纷探讨信息化环境对企业内部控制要素的影响、信息化环境下内部控制的构建等，并认为应该利用信息技术来构建与完善内部控制系统。信息化环境下内部控制系统的变化，必然导致内部控制规范的变化，不论是美国内部控制规范体系中的COSO框架、SOX法案、SEC发布的《最终规则》、COBIT，还是日本的《财务报告内部控制的评价和监督准则》等规范，都充分地考虑了信息化环境对内部控制的影响。面对信息化环境下内部控制及其规范的变化，评价内部控制有效性的内部控制审计就必须考虑信息化环境的影响，从而就产生了信息化内部控制审计的问题。

内部控制审计考虑信息化环境的影响始于上世纪80年代。本世纪以来，各国又陆续出台了一系列相关的规范。如，美国上市公司会计监督委员会（PCAOB）于2004年3月发布了第2号审计准则《与财务报表审计协同进行的财务报告内部控制审计》（简称AS NO.2）。随后，PCAOB于2007年5月又颁布了第5号审计准则《与财务报表审计相结合的财务报告内部控制审计》（简称AS NO.5）以取代AS NO.2。此外，美国注册会计师协会（AICPA）为了与AS No.5保持一致，于2008年发布了鉴证准则第15号（SSAE No. 15）。SOX法案302条款和404条款中的实质性条款也直接影响到了PCAOB、AICPA等对内部控制审计的相关规范。从AS NO.2到AS NO.5，其内容都涉及到IT环境下的内部控制问题。AS NO.5对于IT的应用表现出了更多的关注，如必须评价IT使用的范围，必须认真评估IT对财务报告的影响及其带来的风险等。日本为体现IT的重要性，直接将“对IT的应用”作为内部控制的一个基本组成部分。

我国审计对信息化环境的关注最早体现在审计署发布的相关规范中。1993年，我国审计署发布了《关于计算机审计的暂行规定》，1996年又发布了《审计机关计算机辅助审计办法》，从而拉开了我国IT在审计领域应用的序幕。1999年，中国注册会计师协会发布了《独立审计具体准则第20号——计算机信息系统环境下的审计》，要求注册会计师应充分关注IT环境对被审计单位会计信息及内部控制的影响。2003年6月，中国内部审计协会发布实施了《内部审计具体准则——内部控制审计》，其中要求内部审计人员应评价组织获取及处理信息的能力。2006年，财政部发布了《审计准则第1211号——了解被审计单位及其环境并评估重大错报风险》，认为内部控制应包括自动化成分，在风险评估以及设计和实施进一步审计程序时，应当考虑自动化特征及其影响；还应当从信息技术和人工系统中，对交易生成、记录、处理和报告的程序了解与财务报告相关的信息系统。2007年，财政部发布了《审计准则第1633号——电子商务对财务报表审计的影响》，认为注册会计师应当考虑被审计单位在电子商务中运用的与审计相关的内部控制。2008年，财政部等五部委联合发布了《内部控制审计指引》，认为应当关注信息系统对内部控制及风险评估的影响。2011年10月，中国注册会计师协会发布了《企业内部控制审计指引实施意见》，认为内部控制审计要考虑信息技术控制环境的影响。

（二）信息系统审计　信息系统审计源于EDP（Electronic Data Processing）审计，信息系统审计方面最早的文献是当时主要的计算机制造商IBM公司出版的《电子数据处理审计》和《内部电子处理和审计轨迹》等。这些文献充分考虑了电子数据环境对数据处理流程的影响，提出了许多新的概念、术语和审计技术。

信息系统审计相关准则及规范的颁布进一步推动了信息系统审计理论与实务的不断发展。首先是国际会计师联合会颁布的一系列国际审计准则，包括1984年颁布的国际审计准则第15号《电子数据处理环境下的审计》、国际审计准则第16号《计算机辅助审计

技术》；1985年颁布的国际审计准则第20号《电子数据处理环境对会计制度和有关内部控制研究与评价的影响》；2004年颁布的国际审计准则第401号《计算机信息系统环境下的审计》等。在众多规范中，影响最大的是国际信息系统审计协会（ISACA）制定的信息系统审计准则。其信息系统审计准则体系由标准、指南和程序等3个层次组成，截至2010年1月，ISACA共发布了16个审计标准、42个审计指南和11个审计程序。

我国有关信息系统审计的规范相对比较零散。审计署于1993年发布了《关于计算机审计的暂行规定》，1996年又发布了《审计机关计算机辅助审计办法》；中国注册会计师协会于1999发布了《独立审计准则第20号——计算机信息系统环境下的审计》，2007发布了《审计准则第1633号——电子商务对财务报表审计的影响》；国务院于2001年下发了《关于利用计算机信息系统开展审计工作有关问题的通知》；2004 年，审计署在《2004至2007年审计信息化发展规划》中明确提出了要积极探索信息系统审计，2008 年，《审计署2008 至2012 年信息化发展规划》再一次提出要探索符合我国国情的信息系统审计；2008年，我国内部审计协会发布了《内部审计具体准则第28号——信息系统审计》，这是我国发布的唯一专门针对信息系统审计的准则，开创了我国信息系统审计准则制定的先河。

信息化内部控制审计与信息系统审计分属不同的审计范畴，但却同时对信息技术的应用和内部控制的有效性予以关注。因此，深入剖析信息化内部控制审计与信息系统审计的联系与区别，对整合审计资源有着重要的意义。

二、信息化内部控制审计与信息系统审计的联系

财务报告信息是会计信息系统的产物，会计信息系统的有效运行依赖于内部控制的有效性。在信息化环境下，信息系统审计关注信息技术的应用与信息系统运行的有效性，信息化内部控制审计关注信息技术的应用与内部控制的有效性，因此，信息化内部控制审计和信息系统审计存在着多方面联系。

（一）最终目标一致　PCAOB 的AS NO.5中明确规定，财务报告内部控制审计的目标“是对公司财务报告内部控制的有效性发表意见”。我国《企业内部控制审计指引》也指出，财务报告内部控制审计的目标是内部控制的“有效性”。根据《企业内部控制基本规范》（2010）的相关规定，“有效性”包括制度设计有效性和制度运行有效性两个方面。

ISACA的信息系统审计准则借助COB IT 的“控制目标汇总”表确定各个IT 过程的具体审计目标。我国《内部审计具体准则第28号——信息系统审计》明确指出，信息系统审计的目的是对组织是否达成信息技术管理目标进行综合评价，协助组织信息技术管理人员有效地履行其受托责任以达成组织的信息技术管理目标。

表面看来，信息系统审计与信息化内部控制审计的目标并不一致，但两者的最终目的是一致的，都是合理保证报表使用者得到真实可靠的财务信息。而且，信息系统审计目标的确定很大程度上都与内部控制密切相关。这是因为，财务报告是信息系统的产物，信息系统的运行依赖于内部控制的有效。所以，内部控制的有效性，是为了信息系统的有效运行，是为了最终财务报告信息的质量。

（二）业务类型一致　内部控制审计和信息系统审计都属于基于责任方认定的合理保证鉴证业务。在财务报告内部控制审计业务中，管理层要先评估公司财务报告内部控制的有效性，然后注册会计师再对管理层的评估进行审计，这正是合理保证鉴证业务的范畴。我国《企业内部控制审计指引》中规定，“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也是基于责任方认定的鉴证业务。

信息系统审计的主要任务，是以独立第三方的身份对被审计单位信息系统发表意见，这种意见明显属于合理保证鉴证业务的范畴。COBIT 框架明确提出，“管理层的责任是保护企业的所有资产，为履行这一责任，管理层应建立起一套完善的内部监控体系”。信息系统审计准则正是ISACA基于COBIT的思想建立的监控体系，其目的也是要对管理层的责任认定进行鉴证。我国《内部审计具体准则第28号——信息系统审计》认为信息系统的开发、运行和维护以及信息技术相关的内部控制的设计、执行和监控是组织及其相关人员的责任，实施信息系统审计工作并出具审计报告是信息系统审计人员的责任。这一规定同样说明了信息系统审计属于基于责任方认定的合理保证鉴证业务。

（三）风险导向审计模式的应用　为了充分考虑IT环境的影响，PCAOB 发布的AS NO.2和AS NO.5要求进行内部控制审计时采用自上而下的审计方法，其中AS NO.5称之为风险基础的自上而下审计法，即风险导向的审计模式。我国《企业内部控制审计指引》的亮点之一就是特别强调了风险导向审计思想，根据《企业内部控制审计指引》的规定，注册会计师按照自上而下的方法实施审计工作，并将其作为识别风险、选择拟测试控制的基本思路，这同样是风险导向审计模式的思想。

信息系统审计同样关注风险导向审计模式的应用。在ISACA发布的信息系统审计准则中，与风险评估有关的审计标准有《S11：风险评估在审计计划中的应用》，审计指南有《G13 :风险评估在审计计划中的应用》，审计程序有《P1：信息系统风险评估方法》、《P5 :控制风险自我评估》等。胡晓明（2007）认为，信息系统审计是信息系统风险防范的新途径，应该实施风险导向的信息系统审计。我国《内部审计具体准则第28号——信息系统审计》专门讨论信息系统审计中对信息技术风险的评估，同样体现了风险导向审计的思想。

（四）审计程序相互关联，工作成果能够相互利用　COSO框架认为，信息与沟通是内部控制的五个要素之一，自然是内部控制审计的关注点。而信息与沟通主要通过信息系统实现，与现代信息技术相结合的信息系统具有开放化、实时化、电子化的技术特点，从而影响到内部控制审计的规范实施。所以，在信息化生态环境下，内部控制要解决两个层面的问题，一个是信息化环境下的业务内部控制问题，另一个是其中的信息系统的内部控制问题。在信息化环境下，安全审计应该成为内部控制审计的内容之一。COBIT作为一个综合内部控制模型，既能够适应IT治理需要，又可以确保信息与信息系统的完整性，从而成为内部控制审计和信息系统审计共同的思想基础。PCAOB 的AS NO.2和AS NO.5都强调应该在内部控制审计过程中充分注意信息系统的作用。日本的《财务报告内部控

制的评价和监督准则》也指出，要确保企业内部的信息处理系统能恰当地搜集和处理在各业务领域的数据并能反映在财务报告中。我国《内部审计具体准则——内部控制审计》认为保证管理信息系统的有序运行，保证管理信息系统的安全可靠是内部控制审计过程中必须关注的内容。

信息系统审计通常要包括信息系统内部控制审计，在ISACA发布的信息系统审计准则中，与内部控制直接相关的审计标准有《S15：IT控制》，审计指南有《G11：广泛的信息系统控制的效果》、《G16：在组织的IT控制中第三方的作用》、《G36：生物控制》、《G38：存取控制》，审计程序有《P9：密码方法在管理控制中的评价》、《P10：商业应用改变控制》等。我国《内部审计具体准则第28号——信息系统审计》也认为信息系统审计包括对组织层面信息技术控制、信息技术一般性控制及业务流程层面相关应用控制的审计。

因此，内部控制审计和信息系统审计的很多审计程序相互关联，工作成果能够相互利用。在内部控制审计中发现的控制缺陷能为注册会计师在信息系统审计中认定重点实施审计指明方向。在信息系统审计中对信息系统内部控制的关注可以作为内部控制审计的基础。

三、信息化内部控制审计与信息系统审计的区别

内部控制审计重在“控制有效性”，信息系统审计重在“系统有效性”。因此，二者的审计对象、审计重点等还是存在着差异。

（一）审计对象与内容不同　内部控制审计的对象是企业的内部控制，内部控制审计的内容主要包括内部控制制度的建立、内部控制制度的实施以及内部控制制度实施过程中的监管等方面。根据内部控制一般框架理论，内部控制审计的对象还应包括内部控制的众多影响因素，如内部控制的环境等。信息系统的审计对象是企业的信息系统。信息系统是个比较大的范畴，其内容主要包括信息系统的开发与采纳、信息系统的实施、信息系统的控制、信息系统的维护与评价等。与内部控制审计的对象比较，信息系统审计要包含信息系统内部控制的相关内容，而信息系统化内部控制审计除了关注信息系统的内部控制之外，还要关注企业其他方面的内容控制问题，所以，二者的审计对象与内容有所交叉，但还是有明显的区别。

（二）对内部控制的关注程度不同　首先，从目的性来看，二者对内部控制关注的目的不同。信息系统审计中评价内部控制的目的，是为了判断是否可以相应减少实质性程序的工作量；内部控制审计中评价内部控制的目的，则是为了对内部控制本身的有效性发表审计意见。其次，从内部控制测试范围来看，二者关注的内部控制的范围也不同。信息系统审计可以绕过内部控制测试程序进行审计，而内部控制审计则不能绕过内部控制测试程序进行审计，注册会计师必须针对每一审计领域获取控制有效性的证据，以便对内部控制整体的有效性发表意见。此外，在信息系统审计中，对控制测试的可靠性要求相对较低，而在内部控制审计中，对控制测试的可靠性要求较严。

（三）对控制缺陷的评价要求不同　在内部控制审计中，注册会计师需要对内部控制缺陷进行严格的评估，并区分出重大缺陷，因为重大缺陷将影响到审计意见的类型。而在信息系统审计中，注册会计师仅需区分出值得关注的内部控制缺陷和一般缺陷。

（四）出具的审计报告不同　在信息系统审计中，注册会计师主要是对信息系统的安全、可靠、有效和效率以及能否有效地组织资源，实现组织目标等发表审计意见。在内部控制审计中，注册会计师对内部控制整体的有效性发表意见。信息系统审计是对信息系统的合理鉴证，内部控制审计是对内部控制有效性的合理鉴证。

四、结论

PCAOB的AS NO.5首次提出整合审计的模式，认为财务报告审计与内部控制审计应进行整合。我国《企业内部控制审计指引》明确指出，“注册会计师可以单独进行内部控制审计，也可将内部控制审计与财务报表审计整合进行”。因为整合审计既可以提高上市公司财务信息的质量，又能提高审计效率，降低审计风险，所以，整合审计是一种经济可行、切实兼顾了社会公众、被审计单位和注册会计师行业三者利益的制度安排。

财务报告信息产生于企业的会计信息系统，而内部控制又是保证会计信息系统能够有效运行，从而保证企业财务报告真实、完整的内在机制。内部控制与信息系统之间的必然联系，以及信息技术的广泛应用，使得信息化内部控制审计与信息系统审计之间的联系成为主要的、必然的联系。既然二者的审计模式、程序、方法等存在着相同之处，二者的基础工作可以共享，在一项审计中发现的问题还可以为另一项审计提供线索和思路，那么就不得不考虑信息系统审计、内部控制审计与财务报告审计的关系问题。在信息化环境下，应该把信息系统审计、内部控制审计和财务报告审计进行整合，建立起完善的整合审计体系，以保证财务报告信息的质量。

参考文献：

[1] 陈杰、黄正瑞：《网络环境下会计系统的安全审计》，《会计研究》2000年第1期。

[2] 陈志斌：《信息化生态环境下企业内部控制框架研究》，《会计研究》2007年第1期。

[3] 刘志远、刘洁：《信息技术条件下的企业内部控制》，《会计研究》2001年第12期。

[4] 骆良彬、张白：《企业信息化过程中内部控制问题研究》，《会计研究》2008年第5期。

[5] 谢晓燕、张龙平、李晓红：《我国上市公司整合审计研究》，《会计研究》2009年第9期。

[6] 章铁生：《信息技术条件下的内部控制规范：国际实践与启示》，《会计研究》2007年第7期。

[7] 胡晓明：《风险导向信息系统审计及其发展思路》，《经济管理》2007年第2期。

[8] ISACA. Standards，Guidelines，and Tools and Techniques for Audit/Assurance and Control Professionals. http://www.isaca.org/KNOWLEDGECENTER/STANDARDS/Pages/default.aspx.

[9] PCAOB. AS No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements.http://pcaobus.org/Standards/Auditing/Pages/default.aspx.

（编辑　熊年春）