审计理论研究

高校管理信息系统审计及其风险控制问题研究
——以 WSR 方法论与 COBIT 理论相结合为视角

王会金

（南京审计学院，江苏 南京 211815）

[摘 要]当前，我国高校管理信息系统涉及教务、人事、科研等一系列管理模块，规模相对庞杂，系统安全性、机密性受到挑战，也因此相应地对高校管理信息系统的审计及其风险防范提出了更高的要求。在阐述 WSR 方法论与 COBIT 理论的基础上，首先，基于 WSR 方法论有效设计高校管理信息系统审计的思路与策略；其次，将 WSR 与 COBIT 理念融合于一体，构架高校管理信息系统审计风险控制模型；最后，结合前两步，提出高校在管理信息系统审计及其风险控制中应该注意的问题，力求促进高校管理信息系统在功能实施中更为安全和高效。

[关键词]高校管理信息系统；信息系统审计；WSR 方法论；COBIT 理论；审计风险控制；内部审计

[中图分类号]F239.1 [文献标识码]A [文章编号]1004－4833(2014)05－0023－08

管理信息系统是一个具有高度复杂性、多元性和综合性的人机系统，它全面使用现代计算机技术、网络通信技术、数据库技术，以及管理学、运筹学、统计学、模型论和各种最优化技术，为经营管理与组织决策服务[1]。高校是人才、知识、资产与技术等资源的集聚地，高校之所以设计并实施管理信息系统，其实质就是全面实现高校管理的数字化、信息化、网络化以及科学化，以便能够及时、快捷地组织各项活动，准确做出决策。高校管理信息系统由一系列管理模块构成，如教务管理模块、人事管理模块、科研管理模块、资产管理模块、学生管理模块、财务管理模块、图书管理模块、后勤管理模块等，系统内模块与模块之间彼此协同，共同构筑成一个有机整体。高校管理信息系统的构建是一项庞杂的系统工程，它涉及高校运营的每一方面，且各方面之间存在着杂乱的勾稽关系。所谓高校管理信息系统审计是指 IT 审计师依据特定的审计规范，运用科学系统的程序方法，对高等院校管理信息系统的运行规程与应用对策所实施的一种监督活动，旨在增强高校管理信息系统整体及其各个模块的有效性、安全性、机密性与一致性。高校管理信息系统审计属于中观信息系统审计的范畴。与微观信息系统相比，中观信息系统所涉及的范围广且对象繁多，同时，区域内纷乱的组成个体之间盘节着错综的契约关系，若中观信息系统出现问题，其危害程度远远甚于微观信息系统[2]。有鉴于此，高校应该重视管理信息系统的安全性审计问题，并能够对相应的审计风险做出合理的估计与控制，以便有效规避管理信息系统所带来的各类风险，高效发挥系统各项功能。

一、相关理论追溯

（一）WSR 方法论

物理—事理—人理方法论（Wuli-Shili-Renli Approach），简称 WSR 方法论。该方法论是由顾基发与许志昌两位教授于 1994 年在英国 Hull 大学提出的一种东方系统方法论。WSR 方法论认为，“物

[收稿日期]2014－03－11

[基金项目]江苏高校哲学社会科学重点研究基地重大项目（2012JDXM010）；教育部人文社科研究规划基金项目（14YJA790032）；江苏高校优势学科建设工程二期项目

[作者简介]王会金（1962— ），男，浙江东阳人，南京审计学院副校长，教授，博士，从事审计理论与实务研究。

理”指涉及物质运动的机理,通常要用自然科学知识,主要回答“物”是什么,“物理”需要的是真实性,研究客观存在[3]。“物理”的实质是客观物质世界的规则,其回答的问题是“是什么”,其涉列的原则是追求事物的真相,其解决问题的思路是需要对事物进行功能分析。WSR 方法论认为,“事理”指做事的道理,主要解决如何去安排所有的设备、材料、人员等资源[3]。“事理”的实质是处理事情与实施管理的流程,其回答的问题是“怎样做”,其涉列的原则是保证做事的正确性,其解决问题的思路是需要对事物进行逻辑分析。WSR 方法论认为,实践中处理任何“事”和“物”,以及评价“事”和“物”是否“应用得当”,都必须由人来履行。“人理”指要用人文与社会科学的知识去回答“最好怎么做”的问题,“人理”的作用可以反映在世界观、文化和情感等方面,特别表现在人们处理一些“事”和“物”时的价值观上[3]。实践中的任何做事活动都是“物理”、“事理”和“人理”三者的动态统一。一味地强调“物理”和“事理”,摒弃“人理”,做事不免机械,缺少协调与变通,难有整合与创新。一味地关注“人理”而忽略“物理”和“事理”,则不免偏离事物的本质,适得其反。多年来,WSR 方法论在实践中得到了广泛的应用。WSR 方法论的应用体现在两个方面:(1)资源管理方面。佟雪铭基于 WSR 方法论构建了人力资源管理“物理因素”、“事理因素”、“人理因素”的三维体系和绩效函数模型[4]。顾基发以 WSR 方法论为基础,建立了水资源决策支持系统 WSR 工作图,并设计了水资源管理决策方案[5]。高小慧等提出将 WSR 方法论应用于项目群管理中,构架完整的项目群管理系统,以协调项目群建设中各个方面的关系[6]。(2)战略制定方面。李丰祥和宋杰基于 WSR 思想提出了设计社区体育空间优化战略的建设性思路[7]。王沙骋、赵澄谋、姬鹏宏以 WSR 为视角,将军事情报分析方法体系划分为物理层、事理层和人理层分析方法,并将 WSR 思想融入军事情报分析流程[8]。近年来,关于如何将 WSR 方法论有效应用于审计理论与审计实践的相关研究成果尚缺。

(二) COBIT 理论

1996 年,COBIT 理论第一次由美国信息系统审计与控制协会(ISACA)提出。2012 年 4 月,COBIT 模型已经拓展至第五版本。近年来,COBIT 模型已经逐步演变成为全球学者公认的最为先进、最为权威的安全与信息技术管理和控制的标准体系。经过多年的改进与优化,如今 ISACA 已经将 COBIT5.0 版本打造成为一个治理和管理组织信息系统的成熟业务框架,这也将会更好地帮助企业实现治理和管理组织信息系统的目标。COBIT 模型由执行概要(Executive Summary)、框架(Framework)、执行工具集(Implementation Tool Set)、管理指南(Management Guidelines)、控制目标(Control Objectives) 和审计指南(Audit Guidelines)六个部分构成[9]。COBIT 5.0 在优化以往版本的基础上,吸收国际上其他先进的 IT 治理标准与技术规范,尤其吸收了 ITIL 标准。COBIT 4.1 版本遵循的是“业务为中心、流程为导向、控制为基础、计量为驱动”的理念,而 COBIT 5 版本则倡导“原则为基础、目标为导向、评价为手段、促进因素为载体”的思想[10]。COBIT 5.0 新加入的促进因素具体涵盖了关键流程、组织架构、文化内涵、信息基础设施及应用、人力资源与能力等类项。近年来,COBIT 理论已经被应用在一百六十多个国家的重要组织中。在我国,学者也尝试将 COBIT 理论应用于不同领域。如陈建军结合 COBIT 理论建立了知识管理系统的有效评价模型[11]。刘振海等尝试如何将 COBIT 理论植入央行信息技术审计标准建设之中[12],等等。近年来,将 COBIT 1.0 – COBIT 4.1 版本应用于信息系统内控或审计的研究成果较多,但自 COBIT 5.0 版本发布以来,针对新变化,如何将 COBIT 5.0 应用于信息系统审计及其风险控制的研究成果较少,还有待于学界的继续努力。

二、高校管理信息系统审计策略的 WSR 三维分析

(一) 高校管理信息系统审计的“物理层”分析

高校管理信息系统属于中观信息系统范域,因此,高校管理信息系统秉承了中观信息系统的特性及内涵。高校管理信息系统是由教务、学务、团务、人事、科研、财务、后勤等高校组成部门所属的信息

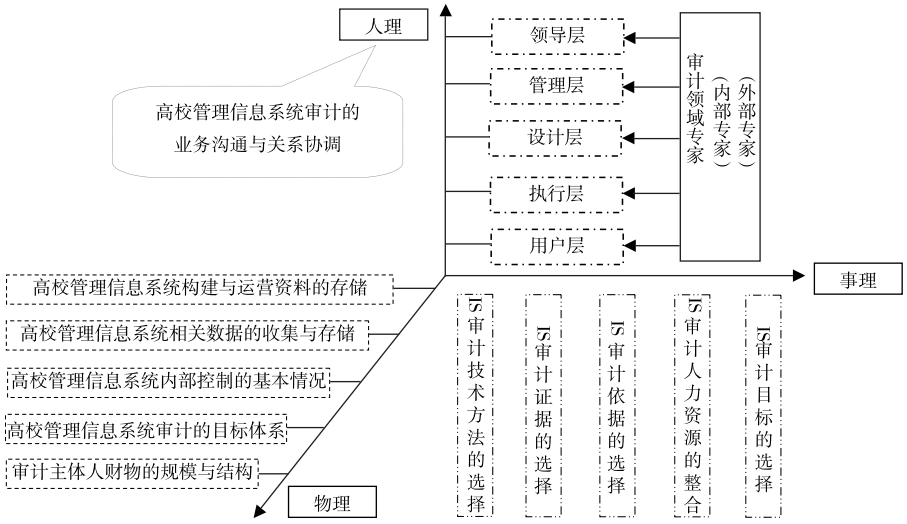

图1　高校管理信息系统审计的WSR三维构架图

资源（如硬件、软件、传输设备、程序、数据以及经验）在高校的统一部署下，以Internet为依托，按照一定的契约规则实施、共享的系统。高校信息系统具有超越单个部门边界、运行繁杂交错、高度依赖网络支持、安全程度要求相对较高等特征。鉴于上述特征，高校对自身管理信息系统审计的要求相对较高。高校管理信息系统审计“物理层”研究的是IS审计人员在高校管理信息系统审计全过程中所面对的“既定现实”。这种“既定现实”是一种客观存在，研究“目前的状态是什么”的问题，它不以人的主观意志为转移。若想高质量地实施高校管理信息系统审计，无论是高校内部的IS审计人员还是外来的IS审计师，都必须能够清晰透彻地认清高校管理信息系统审计的“物理层”，即所面对的审计环境与审计客观条件。当然，“物理层”涉列的因素不仅来自管理信息系统自身，还来自审计主体自身，二者缺一不可。我们对高校管理信息系统审计的“物理层”设计如图1与图2所示，主要包括：（1）高校管理信息系统审计的目标体系组成；（2）高校信息系统内部控制的基本情况，内部控制制度的设计是否科学全面，内部控制制度的执行是否正确有效；（3）高校管理信息系统最初的建设资料是否有所存储，存储是否全面，运行全过程执行材料是否完备；（4）高校管理信息系统在实时运营中自动生成

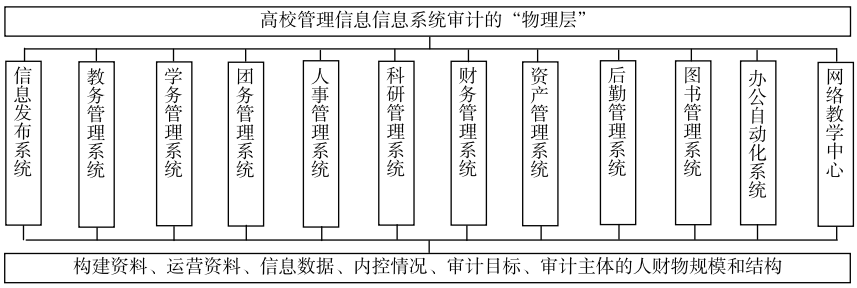

图2　高校管理信息系统审计的“物理层”设计图

的数据信息（如日志数据）保存是否完整；（5）当前的IS审计团队的状态，IS审计人员中是否有现代计算机技术、网络通信技术、数据库技术，以及管理学、统计学等相关领域的专家，而且各领域相关专家的审计经验如何，知识层次如何，针对特定IS审计项目相关专家在审计时间需求上的满足程度如何。上述五方面是高校IS审计主体所必须面对的客观实际，也是他们必须透彻把握的客观物质世界。只有切实把握了客观物质世界，IS审计主体才能真正实现对高校管理信息系统运行规程与应用政策的有效监督。

(二)高校管理信息系统审计的“事理层”分析

高校管理信息系统审计的“事理层”设计见上页图1,具体内容包括以下几个方面。(1)在“既有”的高校管理信息系统审计目标体系中,针对“某一次”或“某一阶段”特定的审计活动,“怎样去选择”科学的信息系统审计总目标与所属的分目标,如究竟是以审查“财务管理系统”的合规性与合法性为目标?还是以审查“科研管理系统”文档资料的完整性为目标?(2)在“现有”的审计人力资源条件下,针对特定的审计项目与具体的审计目标,“怎样去配置”合理的IS审计团队。如“学务管理系统”承载着大学生的教育管理、心理咨询、成长资助、学习支持、招生就业等方面的实时网络服务功能,因而,针对“学务管理系统”开发审计,IS审计团队在配置团队成员时需要考虑是否应该增加本学校学务部门的专家?是否需要再增加此方面成熟运转的其他高校学务部门领域的专家?对这些问题的选择会从根本上弥补审计的不足,拓展审计策略与建议。(3)在“既有”的高校信息系统内外部审计依据体系中,“怎样去选择”适合的审计依据。审计依据是IS审计师衡量被审计高校管理信息系统是非优劣的准绳。IS审计的依据可以是IS法律法规,可以是学校的规章制度,也可以是相关计划与合同或相关业务规范。当前,我国有关于信息系统审计的法律法规较少,且不够深入,高校针对自身所制定的具体的信息系统控制规范与审计标准也较为缺乏。在这样的现实背景下,审计依据的“选择”与“补充”至关重要。(4)在“既定”的高校管理信息系统内外部审计环境下,“怎样去获取”以及“怎样去遴选”审计证据。IS审计不同于传统的审计,IS审计证据更加具有隐蔽性、难以辨认性。因此,如何通过实地观察、日志筛选、言辞陈述与环境事实,基于经验判断甄选审计证据,是出具IS审计结论的必要条件。(5)在“现有”的审计方法体系下,“怎样去选定”科学的IS审计技术与方法。如针对高校的“办公自动化系统”审计,可选择的方法体系中需要考虑是否应该包含“核对法”、“函证法”、“观察法”、“鉴定法”等诸多方法。高校管理信息系统审计的“事理层”回答的是“应该怎样做”的问题,其精髓是通过经验判断寻找最为合理的做事原则,保证做事的正确与高效。

(三)高校管理信息系统审计的“人理层”分析

WSR蕴含“物理层—事理层—人理层”三维层次,且后一层次是前面层次的延伸,基于此,高校管理信息系统审计的“人理层”也是以“物理层”与“事理层”为基础所进行的延伸。人是“物”的执行者与“事”的运营者。由于“物”与“事”无生命,不附有任何运动属性,因而“阅物”与“处事”都离不开人们之间的活动。所谓“人理”是指处事与处物的价值目标与价值尺度。人理的作用集中表现在利用已有的“物理”和“事理”去组织最佳的综合动态实践活动,从而产生最大的效益[13]。高校管理信息系统审计“人理层”的指导思想是在一定的契约规则下,审计人员在同其他关联主体的交往与协作中,持有良好的价值观,和谐相处,汇聚各方智慧,协调各方关系,以促进高校管理信息系统审计目标的高效实现。依据图1,需要同高校管理信息系统的审计主体和谐协作的其他主体包括:(1)领导层。领导层一般是审计的委托人,IS审计师需要协调好自身与委托人的受托关系,明确执行受托任务。(2)管理层。管理层一般是高校各个信息系统模块所属职能机构的管理者,如“科研管理系统”的管理层应该是科研部门的管理者。IS审计师需要协调好与管理层的关系,这样,审计过程才能平稳顺畅。(3)设计层。设计层是信息系统的设计者,他们熟悉信息系统设计的流程与思路,甚至存储着最初设计资料。IS审计师需要协调好自身与设计层的关系,这样在信息系统开发等审计中,IS审计师将会借用设计层的经验与数据,便捷开展审计活动。(4)执行层。执行层是信息系统运营的执行者,IS审计师需要协调好自身与执行层的关系,关注他们实时处理数据,加强互动,全面搜集“第一手”审计证据。(5)用户层。用户层通过反复实践实现了对信息系统的切身检验。用户层汇集着对系统的真实评价以及更高的期待,IS审计师需要协调好自身与用户层的关系,收集系统功能的不足与改进建议,以出具科学的审计报告,提出完善的审计建议。

三、高校管理信息系统审计风险控制模型的建立与探索

高校管理信息系统审计风险属于中观信息系统审计风险的范畴。结合中观信息系统审计风险的内涵[2]，我们认为，高校管理信息系统审计风险是指IS审计师在对高校管理信息系统的整体或局部进行审计的过程中，由于受到某些不确定因素的影响，使得高校管理信息系统审计结论与客观经济事实产生差异，从而受到相关关系人指控并遭遇经济损失以及声望损失的可能性。IS审计师在实施高校管理信息系统审计的过程中，应该加强对审计风险的控制。且审计风险控制不是例外行为，它是以审计活动的实施为载体，并寓于审计行为之中。COBIT是IT治理框架，是一套成熟的信息技术管理与控制体系。基于COBIT的拓展，本文将WSR方法论与COBIT理论相结合，对高校管理信息系统审计风险的控制问题进行研究，并基于图3作进一步分析。

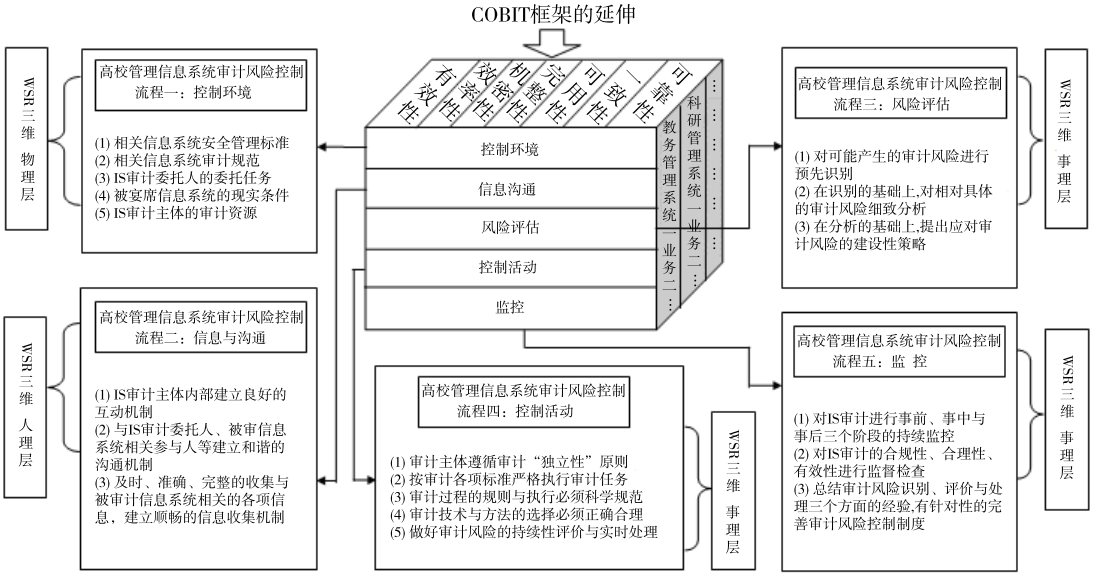

图3　高校管理信息系统审计风险控制模型架构图

（一）高校管理信息系统审计风险控制的COBIT式模型

COBIT 3.0版将IT控制分成了三维空间。第一维空间是IT标准，如质量、信用、安全、可靠与完整；第二维空间是IT资源，包括数据、设备、技术、应用系统以及人力资源；第三维是IT过程，包括4个域、38项控制目标以及相关具体行动。针对高校管理信息系统审计风险控制的特点，图3对COBIT的三维空间进行了延伸，具体分析如下。(1)第一维空间是高校管理信息系统审计目标。图3将COBIT的五项标准演化为七个审计目标，即通过审计加强高校管理信息系统的有效性、效率性、机密性、完整性、可用性、一致性及可靠性。IT标准、信息系统审计目标与信息系统审计风险控制原则三者之间一脉相承。COBIT的IT标准阐释了衡量IT控制的准则，信息系统审计目标阐述了如何依据IT标准获取所期望的成果，信息系统审计风险控制原则阐明了为实现信息系统审计目标所依据的IT准则。因此，高校信息系统审计风险控制的原则与其审计的目标是一致的，最终都是为了实现高校管理信息系统的安全、可用、完整与一致，只有遵循了这样的IT标准，IS审计师的审计结论才不会偏离客观事实，进而才不会受到相关关系人的追控。(2)第二维空间是高校管理信息系统审计具体模块所属相关业务下的资源。图3将COBIT的五项IT资源放入了特定对象之下，这个特定对象就是高校管理信息系统某一具体模块之下的相关业务活动。假定对高校学生“助学贷款”系统的审计风险进行控制，则应该相应地选定“学务管理系统”模块下的“助学贷款”业务活动，且在这个特定对象下分析IT审计及其风险控制所涉及的数据、设备、技术等五项资源。一般而言，IT审计与IT审计风险控制所需的IT资源是一致的，因为两者都是

在同一活动中同步实施的。(3)第三维空间是高校管理信息系统审计风险控制的五项要素。图3的第三维空间并未遵从COBIT理论所提出的“域、过程、任务活动”,而是从另一个角度引入了审计风险控制的“五项要素”,这些要素表现了高校管理信息系统审计风险控制的五个重要过程。

(二)高校管理信息系统审计风险控制的“五项要素”分析

图3模型中第三维度“五项要素”的具体内涵解释如下。(1)控制环境。高校管理信息系统审计风险控制的“控制环境”要素是指围绕“高校管理信息系统审计风险”,并对其控制产生影响的所有外界事物,具体包括:①IS审计及其风险控制所必须遵照的关于信息系统安全的标准、规范与相关制度;②IS审计委托人委托的各项任务;③被审计系统的软硬件条件与应用环境;④IS审计主体的自身条件,如经验、规模、结构等。“控制环境”要素属于WSR方法论中的“物理层”,是IS审计主体在风险控制中所必须面对的客观现实。IS审计师必须全面明晰“审计环境”,这是控制风险的前提。(2)信息和沟通。这一要素属于WSR方法论中的“人理层”,IS审计师有效实施“信息和沟通”过程的关键在于处理好与审计风险控制相关联的其他主体之间的关系,建立良好的内外部沟通机制与顺畅的信息采集机制。(3)风险评估。高校管理信息系统审计风险控制的“风险评估”是指在审计风险事件发生之前或之中,IS审计师通过调查法、决策树法等定量与定性分析方法,对该风险事件的影响或产生损失的可能性进行系列量化评估的过程。这一过程主要包含对审计风险事先的识别、分析、测量与应对等环节。(4)控制活动。“控制活动”是“五项要素”中最为重要的一项要素。高校管理信息系统审计风险控制的“控制活动”贯穿于IS审计的全过程,而且寓于审计之中,审计过程严格、规范、科学必然会大幅度降低审计风险。为降低信息系统审计风险,IS审计师应关注的“控制活动”因素有:①恪守审计“独立性”原则;②执行审计任务时严格遵循各项信息系统安全管理标准与审计规范;③科学规划审计过程;④正确选择审计技术与方法;⑤建立审计风险的实时预警机制;⑥完善审计风险的即时处理机制。(5)监控。高校管理信息系统审计风险控制的“监控”是指对IS审计进行全方位、全过程的监督与检查,并通过对以往风险事件经验的总结,完善审计风险的控制制度。上述五项要素中,“风险评估”、“控制活动”与“监控”属于WSR方法论中的“事理层”,三项要素的执行需要IS审计师的逻辑分析,这就要求IS审计师审时度势,通过缜密的分析找出正确的做事方法。图3中的第三维度是高校管理信息系统审计风险控制的重心,其与第一维度的审计目标、第二维度特定对象业务下的审计资源有机交融,共同构筑了高校管理信息系统审计风险的防御屏障。

四、高校管理信息系统审计及其风险控制的启示与建议

(一)组建健全的高校管理信息系统审计部门与团队

高校管理信息系统属于中观信息系统的范畴,涵盖办公、教学等若干模块,构造庞杂,功能繁多。基于此,高校管理信息系统审计与传统的审计相比,所面临的挑战更大,所涉及的学科已经由传统的审计学拓展成为集计算机科学与技术、网络通信技术、数据库技术、管理学、审计学、统计学、应用数学于一体的交叉学科。由此,高校作为自身管理信息系统审计的委托人,需要从实际出发,统筹规划,成立以信息系统安全、有效、机密、完整、一致为目标的管理信息系统审计专业部门,并组建成熟的IS审计团队。建立部门应该关注的问题如下。(1)部门归属。高校管理信息系统审计应该隶属于高校的内审部门。当前,高校基本上都设置了“审计处(部)”,负责全校的内审工作。我们认为,“审计处(部)”应该专设一个分支机构,负责全校管理信息系统的审计业务。(2)成员构成。高校管理信息系统的审计团队应该遵循多样化原则,建立复合型审计队伍。成员中应该有来自校外实务界的专家,有来自校内各个信息系统模块所属职能机构的资深从业人员,还有来自“审计处(部)”多年从事IS审计实务的审计师,以及最初开发信息系统的专业技术人员等。总之,成员需要保证多学科专业人士有机融合以及系统不同运行阶段参与人的共同配合。(3)团队建设。高校管理信息系统审计团队的建

设是一个长期的过程,成员间专业经历不同,有专兼职的差异和校内外的差异,不便于管理,因而,高校在审计团队建设中必须做好五点内容,即正确的组织领导、共同的事业愿景、清晰的团队目标、科学的激励机制与系统的学习提升,仅有如此,审计团队才能真正发挥信息系统审计的作用,进而为审计风险的控制打下基础。

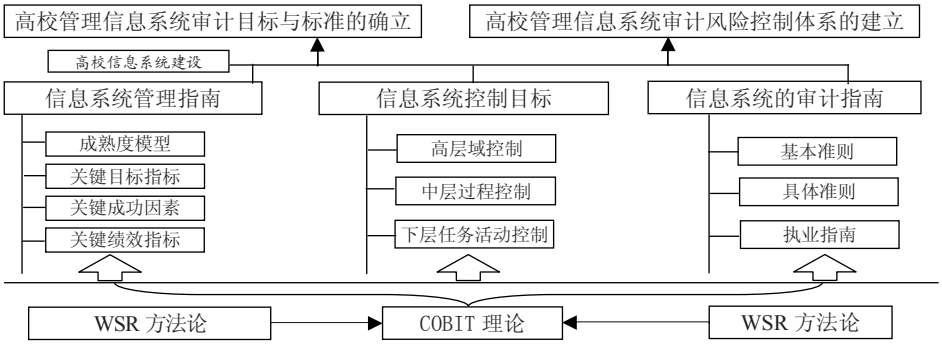

图4　高校管理信息系统审计及其风险控制的体系设计

（二）构架良好的高校管理信息系统审计运行机制

近年来,我国在传统审计上已经形成了成熟的体系标准,然而,在高校管理信息系统审计的准则与规范方面,相关成果相对较少。面对如此现状,尽管高校建立了健全的机构与团队,但因为IS审计师缺少衡量审计质量的尺度,缺乏确定和解脱审计责任的依据,高校管理信息系统的审计及风险控制仍无从谈起。基于此,高校需要引入WSR方法论与COBIT理论等外部理论来构架管理信息系统审计的相关规范与运营流程(图4),通过借助外来理论强化对高校管理信息系统审计的建设。前文所述,COBIT模型由执行概要、框架、执行工具集、管理指南、控制目标与审计指南六部分组成,图4截取了后三部分来对高校管理信息系统的审计运行机制进行研究,并作如下解释。(1)引入COBIT的管理指南。COBIT的管理指南提供了信息系统管理的工具,给出了包括成熟度模型、关键成功因素、关键目标指标、关键绩效指标在内的度量信息系统的指标体系以及评估准则在内的度量模型。IS审计师可以借用相关指标体系与度量模型判断系统的开发是否符合行业标准、判断具体审计业务处理的复杂性、充分关注被审计系统固定风险的具体业务处理事项。(2)引入COBIT的控制目标。COBIT的控制目标包括4个高层域、38项中层控制目标、318项具体活动控制。多方位、多层次的COBIT控制目标弥补了当前高校管理信息系统审计规范的极度匮乏,为IS审计师"怎样评价内控"以及"依据什么审计"提供了绝佳的系列参考样板。(3)引入COBIT的审计指南。COBIT的审计指南涵盖了信息系统审计的基本准则、具体准则与执业指南。审计指南为IS审计师审计高校信息系统规定了审计行为必须达到的基本要求,规定了审计业务实施的具体规范、操作规程与具体方法。依据WSR方法论,高校管理信息系统审计对COBIT模型后三部分的"引入"属于"物理层",COBIT模型中的具体内容是"客观存在",是IT治理的通用性标准,但是,对于COBIT模型后三部分的"吸收"却属于"事理层",它要求审计部门实事求是、去粗取精,采用逻辑分析方法,处好"事",选好"物",实现"事物"的最佳均衡状态。

（三）建立完善的高校管理信息系统审计风险控制体系

传统审计风险模型下,审计风险涵盖固有风险、控制风险与检查风险。面对高校管理信息系统的固有风险、控制风险以及IS审计师的检查风险等,高校有必要建立完善的管理信息系统审计风险控制体系。结合图3与图4,我们可以发现审计风险控制体系的建立并非难事。图3的COBIT式三维框架为我们提供了IS审计风险控制的思路,即针对某一"信息系统模块具体业务活动及其所属的相关资源",按照"7项IT目标",在"五项要素"下结合WSR方法论实现对审计风险的控制。图4中COBIT理论下"管理指南"、"控制目标"为IS审计师挖掘高校信息系统自身的固有风险与控制风险提供了参照样板。如

“管理指南”所属的“关键目标指标”阐释了信息技术处理中最关键环节应实现“什么样”的目标,当 IS 审计师发现“关键理想目标”与“实际处理结果”之间出现严重差异时,IS 审计师可以基于相关原理,进一步考查其固有风险及控制风险,并评价这一“有害事件”的重要程度。另外,图 4“审计指南”中的系列准则对规范 IS 审计师自身的审计行为,以进一步防范检查风险提供了可操作性指导。需要说明的是,当前有部分高校自身并未建立信息系统审计平台,而是采用信息系统审计项目外包的方式[14]。对于这种情形,高校与外来 IS 审计部门都存在着风险,高校的风险是存在重要信息泄露的可能,而外来 IS 审计部门的风险是因缺少高校相关职能部门专业人士的参与而导致不能全面、深入地挖掘被审计系统的固有风险与控制风险。在此,我们建议高校与外包审计部门关注自身风险,并希望外包审计部门尽可能合理融合高校专业人士,组建复合型团队,提高 IS 审计质量,有效防范 IS 审计风险。

参考文献:

[1]张金城. 管理信息系统[M]. 1 版. 北京:北京大学出版社,2001.
[2]刘国城,王会金. 中观信息系统审计风险管理的理论探索与体系构架[J]. 审计研究,2011(2):21 -28.
[3]顾基发,唐锡晋. 物理—事理—人理系统方法论:理论与应用[M]. 1 版. 上海:上海科技教育出版社,2006.
[4]佟雪铭. WSR 方法论在人力资源开发研究中的应用[J]. 软科学,2008(1):135 -138.
[5]顾基发. 物理事理人理系统方法论的实践[J]. 管理学报,2011(3):317 -355.
[6]高小慧,顾基发. 基于 WSR 系统方法论的项目群管理研究[J]. 项目管理技术,2012(10):65 -69.
[7]李丰祥,宋杰. 基于 WSR 思想的城市社区体育空间建设研究[J]. 体育科学,2006(6):43 -46.
[8]王沙骋,赵澄谋,姬鹏宏. 基于 WSR 的军事情报分析[J]. 情报杂志,2007(4):22 -23.
[9]ISACA. About isaca[EB/OL]. http://www. isaca. org/about-isaca/.
[10]鲁清仿. COBIT5 与 COBIT4. 1 的比较与启示[J]. 财会月刊,2014(1):89 -92.
[11]陈建军. 知识管理系统绩效评价研究[J]. 情报杂志,2007(10):18 -21.
[12]刘振海,刘晶,刘海林. 基于 COBIT 的央行信息技术审计标准研究[J]. 金融理论与实践,2012(12):35 -38.
[13]马轶群. 基于 WSR 的政府审计应对非常规事件的管理系统研究[J]. 审计月刊,2010(7):7 -10.
[14]唐文杰. 高校信息系统审计策略探讨[J]. 财会月刊,2012(5):71 -73.

[责任编辑:刘　茜]

Research on Audit and it's Risk Control about Management Information Systems of University ——From the Perspective of Combination WSR Methodology with COBIT Theory

WANG Huijin
(Nanjing Audit University, Nanjing 211815, China)

Abstract: Currently, the management information systems of university involve a series of management modules such as the senate, personnel, and research. Due to its relative complexity, the security and confidentiality are being challenged, accordingly, higher requirements are also put forwarded towards the management information system of university for audit and risk prevention. Based on the elaboration of WSR Methodology and COBIT theory, firstly, ideas and strategies of university management information systems based on WSR are effectively designed, secondly, under the combination of WSR and COBIT concept, audit risk control model of the university management information system is framed, issues on audit and risk control that need to be paid attention in universities management information systems are also put forwarded, in order to promote the university management information systems to be more secure and more efficient in the functional implementation.

Key Words: university management information systems; information systems audit; WSR methodology; COBIT theory; audit risk control; internal audit