审计理论研究

中观信息系统审计风险控制体系研究

——以COBIT框架与数据挖掘技术相结合为视角

王会金

(南京审计学院,江苏 南京 211815)

[摘 要]当前,我国急需一套完善的中观信息系统审计风险控制体系。这是因为我国的中观经济主体在控制信息系统审计风险时需要一套成熟的管理流程,且国家有关部门在制定信息系统审计风险防范标准方面也需要完善的控制体系作为支撑。在阐述COBIT与数据挖掘基本理论的基础上,借鉴COBIT框架,构建中观信息系统审计风险的明细控制框架,利用数据挖掘技术有针对性地探索每一个明细标准的数据挖掘路径,创建挖掘流程,建立适用于我国中观经济特色的信息系统审计风险控制体系。

[关键词]中观信息系统审计;COBIT框架;数据挖掘;风险控制;中观审计

[中图分类号]F239.4 [文献标识码]A [文章编号]1004-4833(2012)01-0016-08

中观信息系统审计是中观审计的重要组成部分,它从属于中观审计与信息系统审计的交叉领域。中观信息系统审计是指IT审计师依据特定的规范,运用科学系统的程序方法,对中观经济主体信息系统的运行规程与应用政策所实施的一种监督活动,旨在增强中观经济主体特定信息网络的有效性、安全性、机密性与一致性[1]。与微观信息系统相比,中观信息系统功能更为复杂,且区域内纷乱的个体间存在契约关系。中观信息系统的复杂性主要体现在跨越单个信息系统边界,参与者之间在信息技术基础设施水平、信息化程度和能力上存在差异,参与者遵循一定的契约规则,依赖通信网络支持,对安全性的要求程度很高等方面。中观信息系统审计风险是指IT审计师在对中观信息系统进行审计的过程中,由于受到某些不确定性因素的影响,而使审计结论与经济事实不符,从而受到相关关系人指控或媒体披露并遭受经济损失以及声誉损失的可能性。中观信息系统审计风险控制的研究成果能为我国大型企业集团、特殊的经济联合体等中观经济主体保持信息系统安全提供强有力的理论支持与实践指导。

一、相关理论概述与回顾

(一)COBIT

信息及相关技术的控制目标(简称COBIT)由美国信息系统审计与控制协会(简称ISACA)颁布,是最先进、最权威的安全与信息技术管理和控制的规范体系。COBIT将IT过程、IT资源及信息与企业的策略及目标联系于一体,形成一个三维的体系框架。COBIT框架主要由执行工具集、管理指南、

[收稿日期]2011-08-21
[基金项目]教育部人文社会科学研究规划项目(10YJA790182);江苏省优势学科"审计科学与技术"研究项目
[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,从事信息系统审计研究。

控制目标和审计指南四个部分组成,它主要是为管理层提供信息技术的应用构架。COBIT 对信息及相关资源进行规划与处理,从信息技术的规划与组织、采集与实施、交付与支持以及监控等四个方面确定了 34 个信息技术处理过程。

ISACA 自 1976 年发布 COBIT1.0 版以来,陆续颁布了很多版本,最近 ISACA 即将发布 COBIT5.0 版。ISACA 对 COBIT 理论的研究已趋于成熟,其思路逐步由 IT 审计师的审计工具转向 IT 内部控制框架,再转向从高管层角度来思考 IT 治理。大多数国际组织在采纳 COSO 框架时,都同时使用 COBIT 控制标准。升阳电脑公司等大型国际组织成功应用 COBIT 优化 IT 投资。2005 年,欧盟也选择将 COBIT 作为其审计准则。国内学者对 COBIT 理论的研究则以借鉴为主,如阳杰、张文秀等学者解读了 COBIT 基本理论及其评价与应用方法[2-3];谢羽霄、黄溶冰等学者尝试将 COBIT 理论应用于银行、会计、电信等不同的信息系统领域[4-5]。我国信息系统审计的研究目前正处于起步阶段,因而将 COBIT 理论应用于信息系统的研究也不够深入。王会金、刘国城研究了 COBIT 理论在中观信息系统重大错报风险评估中的运用,金文、张金城研究了信息系统控制与审计的模型[1,6]。

(二) 数据挖掘

数据挖掘技术出现于 20 世纪 80 年代,该技术引出了数据库的知识发现理论,因此,数据挖掘又被称为"基于数据库的知识发现(KDD)"。1995 年,在加拿大蒙特利尔召开的首届 KDD & Date Mining 国际学术会议上,学者们首次正式提出数据挖掘理论[7]。当前,数据挖掘的定义有很多,但较为公认的一种表述是:"从大型数据库中的数据中提取人们感兴趣的知识。这些知识是隐含的、事先未知的潜在有用信息,提取的知识表现为概念、规则、规律、模式等形式。数据挖掘所要处理的问题就是在庞大的数据库中寻找有价值的隐藏事件,加以分析,并将有意义的信息归纳成结构模式,供有关部门在进行决策时参考。"[7]1995 年至 2010 年,KDD 国际会议已经举办 16 次;1997 年至 2010 年,亚太 PAKDD 会议已经举办 14 次,众多会议对数据挖掘的探讨主要围绕理论、技术与应用三个方面展开。

目前国内外学者对数据挖掘的理论研究已趋于成熟。亚太 PAKDD 会议主办方出版的论文集显示,2001 年至 2007 年仅 7 年时间共有 32 个国家与地区的 593 篇会议论文被论文集收录。我国学者在数据挖掘理论的研究中取得了丰硕的成果,具体表现在两个方面:一是挖掘算法的纵深研究。李也白、唐辉探索了频繁模式挖掘进展,邓勇、王汝传研究了基于网络服务的分布式数据挖掘,肖伟平、何宏研究了基于遗传算法的数据挖掘方法[8-10]。二是数据挖掘的应用研究。我国学者对于数据挖掘的应用研究也积累了丰富的成果,并尝试将数据挖掘技术应用于医学、通讯、电力、图书馆、电子商务等诸多领域。2008 年以来,仅在中国知网查到的关于数据挖掘应用研究的核心期刊论文就多达 476 篇。近年来,国际软件公司也纷纷开发数据挖掘工具,如 SPSS Clementine 等。同时,我国也开发出数据挖掘软件,如上海复旦德门公司开发的 Dminer,东北大学软件中心开发的 Open Miner 等。2000 年以来,我国学者将数据挖掘应用于审计的研究成果很多,但将数据挖掘应用于信息系统审计的研究成果不多,且主要集中于安全审计领域具体数据挖掘技术的应用研究。

二、中观信息系统审计风险控制体系的构想

本文将中观信息系统审计风险控制体系(图 1)划分为以下三个层次。

(一) 第一层次:设计中观信息系统审计风险的控制框架与明细控制标准

中观信息系统审计的对象包括信息安全、数据中心运营、技术支持服务、灾难恢复与业务持续、绩效与容量、基础设施、硬件管理、软件管理、数据库管理、系统开发、变革管理、问题管理、网络管理、中观系统通信协议与契约规则等共计 14 个主要方面[11]。中观信息系统审计风险控制体系的第一层次是根据 COBIT 三维控制框架设计的。这一层次需要构架两项内容:(1)中观信息系统审计风险的控制框架。该控制框架需要完全融合 COBIT 理论的精髓,并需要考虑 COBIT 理论的每一原则、标准、解释及说明。该

控制框架由 14 项风险防范因子组成，这 14 个因子必须与中观信息系统审计的 14 个具体对象相对应。框架中的每一个因子也应该形成与自身相配套的风险控制子系统，且子系统应该包含控制的要素、结构、种类、目标、遵循的原则、执行概要等内容。(2)中观信息系统审计风险的明细控制标准。控制框架中的 14 项风险防范因子需要具备与自身相对应的审计风险明细控制规则，IT 审计师只有具备相应的明细规范，才能在中观信息系统审计实施过程中拥有可供参考的审计标准。每个因子的风险控制标准的设计需要以 COBIT 三维控制框架为平台，以 4 个域、34 个高层控制目标、318 个明细控制目标为准绳。

(二) 第二层次：确定风险控制框架下的具体挖掘流程以及风险控制的原型系统

第一层次构建出了中观信息系统审计风险控制的明细标准 $X_i(i \in 1 \to n)$。在第一层次的基础上，第二层次需要借助于数据挖掘技术，完成两个方面的工作。一是针对 X_i，设计适用于 X_i 自身特性的数据挖掘流程。这一过程的完成需要数据资料库的支持，因而，中观经济主体在研讨 X_i 明细控制标准下的数据挖掘流程时，必须以多年积累的信息系统控制与审计的经历为平台，建立适用于 X_i 的主题数据库。针对明细标准 X_i 的内在要求以及主题数据库的特点，我们就可以选择数据概化、统计分析、聚类分析等众多数据挖掘方法中的一种或若干种，合理选取特征字段，分层次、多角度地进行明细标准 X_i 下的数据挖掘实验，总结挖掘规律，梳理挖掘流程。二是将适用于 X_i 的 n 个数据挖掘流程体系完善与融合，开发针对本行业的中观信息系统审计风险控制的原型系统。原型系统是指系统生命期开始阶段建立的，可运行的最小化系统模型。此过程通过对 n 个有关 X_i 的数据挖掘流程的融合，形成体系模型，并配以详细的说明与解释。对该模型要反复验证，多方面关注 IT 审计师对该原型系统的实际需求，尽可能与 IT 审计师一道对该原型系统达成一致理解。

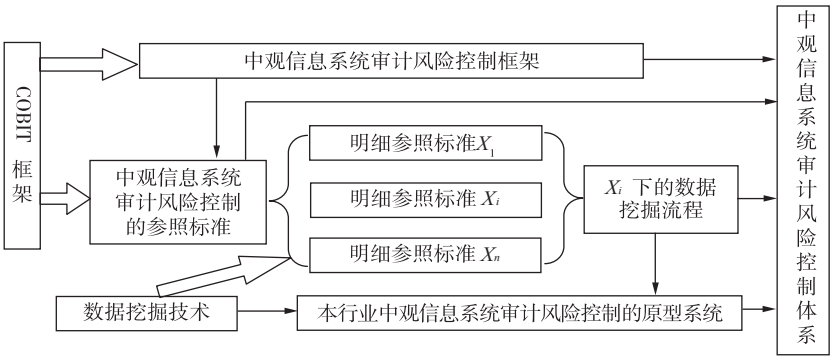

图 1　中观信息系统审计风险控制的体系结构

(三) 第三层次：整合前两个步骤，构建中观信息系统风险控制体系

第三层次是对第一层次与第二层次的整合。第三层次所形成的中观信息系统风险控制体系包括四部分内容：(1)中观信息系统审计风险控制框架；(2)中观信息系统审计风险控制参照标准；(3)中观信息系统审计风险控制明细标准所对应的数据挖掘流程集；(4)目标行业的中观信息系统审计风险控制的原型系统。在此过程中，对前三部分内容，需要归纳、验证、总结，并形成具有普遍性的中观审计风险控制的书面成果；对第四部分内容，需要在对原型系统进行反复调试的基础上将其开发成软件，以形成适用于目标行业不同组织单位的“软性”成果。在设计中观信息系统风险控制体系的最后阶段，需要遵循控制体系的前三部分内容与第四部分内容相互一致、相互补充的原则。相互一致表现在控制体系中的框架、明细控制标准、相关控制流程与原型系统中的设计规划、属项特征、挖掘原则相协调；相互补充表现在控制体系中的框架、明细控制标准及相关控制流程是 IT 审计师在中观信息系统审计中所参照的一般理念，而原型系统可为 IT 审计师提供审计结论测试、理念指导测试以及验证结论。

三、COBIT 框架对中观信息系统审计风险控制的贡献

(一) COBIT 框架与中观信息系统审计风险控制的契合分析

现代审计风险由重大错报风险与检查风险两个方面组成，与传统审计风险相比，现代审计风险拓展了风险评估的范围，要求考虑审计客体所处的行业风险。但从微观层面看，传统审计风险与现代审

计风险的主要内容都包括固有风险、控制风险与检查风险。COBIT 框架与中观信息系统审计风险控制的契合面就是中观信息系统的固有风险与控制风险。中观信息系统的固有风险是指“假定不存在内部控制情况下,中观信息系统存在严重错误或不法行为的可能性”;中观信息系统的控制风险是指“内部控制体系未能及时预防某些错误或不法行为,以致使中观信息系统依然存在严重错误或不法行为的可能性”;中观信息系统的检查风险是指“因 IT 审计师使用不恰当的审计程序,未能发现已经存在重大错误的可能性”。IT 审计师若想控制中观信息系统的审计风险,必须从三个方面着手:(1)对不存在内部控制的方面,能够辨别和合理评价被审系统的固有风险;(2)对存在内部控制的方面,能够确认内部控制制度的科学性、有效性、健全性,合理评价控制风险;(3)IT 审计师在中观信息系统审计过程中,能够更大程度地挖掘出被审系统“已经存在”的重大错误。我国信息系统审计的理论研究起步较晚,IT 审计师在分辨被审系统固有风险,确认控制风险,将检查风险降低至可接受水平三个方面缺乏成熟的标准加以规范,因此我国的中观信息系统审计还急需一套完备的流程与指南①。

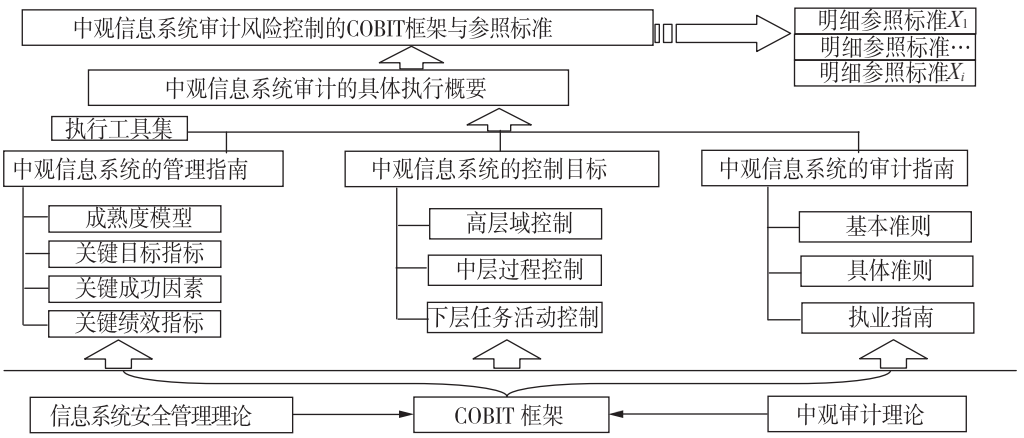

图 2　中观信息系统审计风险的控制框架与控制标准的设计思路

COBIT 框架能够满足 IT 审计师的中观信息系统审计需求,其三维控制体系,4 个控制域、34 个高层控制目标、318 个明细控制目标为 IT 审计师辨别固有风险,分析控制风险,降低检查风险提供了绝佳的参照样板与实施指南。COBIT 控制框架的管理理念、一般原则完全可以与中观信息系统审计风险的控制实现完美契合。通过对 COBIT 框架与中观信息系统审计的分析,笔者认为 COBIT 框架对中观信息系统审计风险控制的贡献表现在三个方面(见图 2):(1)由 COBIT 的管理指南,虚拟中观信息系统的管理指南,进而评价中观主体对自身信息系统的管理程度。COBIT 的管理指南由四部分组成,其中成熟度模型用来确定每一控制阶段是否符合行业与国际标准,关键成功因素用来确定 IT 程序中最需要控制的活动,关键目标指标用来定义 IT 控制的目标绩效水准,关键绩效指标用来测量 IT 控制程序是否达到目标。依据 COBIT 的管理指南,IT 审计师可以探寻被审特定系统的行业与国际标准、IT 控制活动的重要性层次、IT 控制活动的目标绩效水平以及评价 IT 控制活动成效的指标,科学地拟定被审系统的管理指南。(2)由 COBIT 的控制目标,构建中观信息系统的控制目标体系,进而评价中观信息系统的固有风险与检查风险。COBIT 的控制目标包括高层域控制、中层过程控制、下层任务活动控制三个方面,其中,高层域控制由规划与组织、获取与实施、交付与支持以及监控四部分组成,中层控制过程由“定义 IT 战略规划”在内的 34 个高层控制目标组成,下层任务活动控制由 318 个明细控制目标组成。COBIT 的控制目标融合了“IT 标准”、“IT 资源”以及被审系统的“商业目标”,为 IT 审计师实施中观信息系统审计风险控制

①当前我国有四项信息系统审计标准,具体为《审计机关计算机辅助审计办法》、《独立审计具体准则第 20 号——计算机信息系统环境下的审计》、《关于利用计算机信息系统开展审计工作有关问题的通知》(88 号文件)以及《内部审计具体准则第 28 号——信息系统审计》。

提供了层级控制体系与明细控制目标。IT 审计师可以直接套用 COBIT 的控制层级与目标拟定中观信息系统管理与控制的层级控制体系以及明细控制目标,然后再进一步以所拟定的明细控制目标作为参照样板,合理评判中观信息系统的固有风险与控制风险。中观信息系统中“域”、“高层”、“明细”控制目标的三层结构加强了 IT 审计师审计风险控制的可操作性。(3)由 COBIT 的审计指南,设计 IT 审计师操作指南,进而降低中观信息系统审计的检查风险。COBIT 的审计指南由基本准则、具体准则、执业指南三个部分组成。基本准则规定了信息系统审计行为和审计报告必须达到的基本要求,为 IT 审计师制定一般审计规范、具体审计计划提供基本依据。具体准则对如何遵循 IT 审计的基本标准,提供详细的规定、具体说明和解释,为 IT 审计师如何把握、评价中观经济主体对自身系统的控制情况提供指导。执业指南是根据基本标准与具体准则制定的,是系统审计的操作规程和方法,为 IT 审计师提供了审计流程与操作指南。

(二)中观信息系统审计风险控制体系建设举例——构建“设备管理”控制目标体系

前文所述,中观信息系统审计的对象包括“信息安全”等 14 项内容,本文以“硬件管理”为例,运用 COBIT 的控制目标,构建“硬件管理”的控制目标体系,以利于 IT 审计师科学评价“硬件管理”存在的固有风险与控制风险。“设备管理”控制目标体系的构建思路参见表 1。

表 1　中观信息系统中“设备管理”的层级控制目标体系

域控制(4 个方面)		中高层过程控制(21 个方面)	IT 标准							IT 资源					下层任务活动控制(149 个方面)
			有效性	效率性	机密性	完整性	可用性	一致性	可靠性	人员	应用	技术	设备	数据	
规划与组织(P)	P01	定义战略规划	P	S						C	C	C			6 项控制目标
	P05	设备的投资效果	P	P					S	C	C	C		C	6 项控制目标
	P07	人力资源管理	P	P						C					3 项控制目标
	P08	确保与外部需求一致	P					P	S	C	C			C	6 项控制目标
	P011	质量管理	P	P		P			S	C	C	C			7 项控制目标
获取与实施(A)	AI3	维护技术基础设施	P	P		S						C			4 项控制目标
	AI5	设备安装与维护	P			S	S			C	C	C		C	7 项控制目标
	AI6	改善与变革管理	P	P		P	P		S	C	C	C		C	9 项控制目标
交付与支持(D)	DS2	管理第三方的服务	P	P	S	S	S	S	S	C	C	C		C	11 项控制目标
	DS3	管理性能与容量	P	P			S				C	C			5 项控制目标
	DS4	确保服务的连续性	P	S			P			C	C	C		C	7 项控制目标
	DS5	确保设备安全			P	P	S	S	S	C	C	C		C	9 项控制目标
	DS7	教育并培训用户	P	S						C					3 项控制目标
	DS8	协助并为客户提供建议	P	P						C	C				4 项控制目标
	DS9	配置管理	P				S		S		C	C			5 项控制目标
	DS10	处置问题和突发事件	P	P			S			C	C	C		C	7 项控制目标
	DS13	＊运营管理(举例)	P	P		S	S			C	C				6 项控制目标
监控(M)	M1	过程监控	P	P	S	S	S	S	S	C	C	C		C	11 项控制目标
	M2	评价内部控制的适当性	P	P	S	S	S	P	S	C	C	C		C	11 项控制目标
	M3	获取独立性的证明	P	P	S	S	S	P	S	C	C	C		C	11 项控制目标
	M4	提供独立的审计	P	P	S	S	S	P	S	C	C	C		C	11 项控制目标

注:IT 标准对 IT 过程的影响中 P 表示直接且主要的,S 表示间接且次要的;IT 过程所涉及的 IT 资源中 C 表示涉及;空白表示关联微小。

表 1 以“设备管理”为研究对象,结合 COBIT 控制框架,并将 COBIT 框架中与“设备管理”不相关的中层控制过程剔除,最终构建出“设备管理”控制的目标体系。该体系由 4 个域控制目标、21 个中层过程控制目标、149 个明细控制目标三个层级构成,各个层级的关系见表 1。(1)第一层级是域控制,由“P. 设备管理的组织规划目标”、“A. 设备管理的获取与实施目标”、“DS. 设备管理的交付与支持目标”以及“M. 设备管理的监控目标”构成;(2)第二层级是中层过程控制,由 21 个目标构成,其中

归属于 P 的目标 5 个,归属于 A 的目标 3 个,归属于 D 的目标 9 个,归属于 M 的目标 4 个;(3)第三层级是下层任务活动控制,由 149 个明细目标构成,该明细目标体系是中层过程控制目标(P、A、DS、M)针对"IT 标准"与"IT 资源"的进一步细分。IT 标准是指信息系统在运营过程中所应尽可能实现的规则,具体包括有效性、效率性、机密性等 7 项;IT 资源是指信息系统在运营过程中所要求的基本要素,具体有人员、应用等 5 项。根据表 1 中"有效性"、"人员"等"IT 标准"与"IT 资源"合计的 12 个属项,每个具体中层控制目标都会衍生出多个明细控制目标。例如,中层控制目标"DS_{13}. 运营管理"基于"IT 标准"与"IT 资源"的特点具体能够演绎出 6 项明细控制目标,此 7 项可表述为"DS_{13} -01. 利用各项设备,充分保证硬件设备业务处理与数据存取的及时、正确与有效","DS_{13} -02. 充分保证硬件设备运营的经济性与效率性,在硬件设备投入成本一定的情况下,相对加大硬件设备运营所产生的潜在收益","DS_{13} -03. 硬件设备保持正常的运营状态,未经授权,不可以改变硬件的状态、使用范围与运营特性,保证设备运营的完整性","DS_{13} -04. 设备应该在规定条件下和规定时间内完成规定的功能与任务,保证设备的可用性","DS_{13} -05. 硬件设备运营的参与人员必须具备较高的专业素质,工作中遵循相应的行为规范"以及"DS_{13} -06. 工作人员在使用各项硬件设备时,严格遵循科学的操作规程,工作中注意对硬件设备的保护,禁止恶意损坏设备"。上述三个层级组成了完整的"硬件设备"控制目标体系,若将中观信息系统审计的 14 个对象都建立相应的控制目标体系,并将其融合为一体,则将会形成完备的中观信息系统审计风险控制的整体目标体系。

四、数据挖掘技术对中观信息系统审计风险控制的贡献

(一) 数据挖掘技术与中观信息系统审计风险控制的融合分析

中观信息系统是由两个或两个以上微观个体所构成的中观经济主体所属个体的信息资源,在整体核心控制台的统一控制下,以 Internet 为依托,按照一定的契约规则实施共享的网状结构式的有机系统。与微观信息系统比较,中观信息系统运行复杂,日志数据、用户操作数据、监控数据的数量相对庞杂。因而,面对系统海量的数据信息,IT 审计师针对前文所构建的明细控制目标 X_i 下的审计证据获取工作将面临很多问题,如数据信息的消化与吸收、数据信息的真假难辨等。而数据挖掘可以帮助决策者寻找数据间潜在的知识与规律,并通过关联规则实现对异常、敏感数据的查询、提取、统计与分析,支持决策者在现有的数据信息基础上进行决策[12]。数据挖掘满足了中观信息系统审计的需求,当 IT 审计师对繁杂的系统数据一筹莫展时,数据挖掘理论中的聚类分析、关联规则等技术却能为中观信息系统审计的方法提供创新之路。笔者认为,将数据挖掘技术应用于前文所述的明细控制目标 X_i 下审计证据筛选流程的构建是完全可行的。恰当的数据挖掘具体技术,科学的特征字段选取,对敏感与异常数据的精准调取,将会提高中观信息系统审计的效率与效果,进而降低审计风险。

(二) 中观信息系统审计风险控制目标 X_i 下数据挖掘流程的规划

数据挖掘技术在中观信息系统审计风险控制中的应用思路见图 3。中观信息系统审计明细控制目标 X_i 下数据挖掘流程设计具体可分为六个过程:(1)阐明问题与假设。本部分的研究是在一个特定的应用领域中完成的,以"中观信息系统审计风险明细控制目标 X_i"为主旨,阐明相关问题、评估"控制目标 X_i"所处的挖掘环境、详尽的描述条件假设、合理确定挖掘的目标与成功标准,这些将是实现"控制目标 X_i 下"挖掘任务的关键。(2)数据收集。图 3 显示,本过程需要从原始数据、Web 记录与日志文件等处作为数据源采集数据信息,采集后,还需要进一步描述数据特征与检验数据质量。所采集数据的特征描述主要包括数据格式、关键字段、数据属性、一致性,所采集数据的质量检验主要考虑是否满足"控制目标 X_i"下数据挖掘的需求,数据是否完整,是否存有错误,错误是否普遍等。(3)数据预处理。该过程是在图 3 的"N. 异构数据汇聚数据库"与"U. 全局/局部数据仓库"两个模块下完成的。N 模块执行了整合异构数据的任务,这是因为 N 中的异构数据库由不同性质的异构数据组

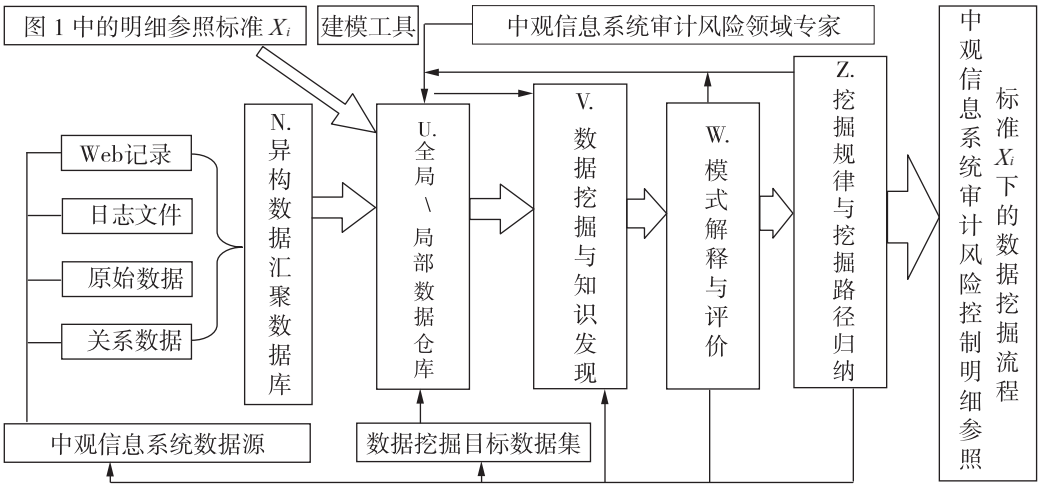

图3　数据挖掘在中观信息系统审计风险控制中的应用思路

注:数据仓库具体为目标行业特定中观经济主体的信息系统数据库

合而成,数据属性、数据一致性彼此间可能存在矛盾,故N模块需要通过数据转换与数据透明访问实现异构数据的共享。U模块承载着实现数据清理、数据集成与数据格式化的功能。“控制目标 X_i”下的数据挖掘技术实施前,IT审计师需要事先完成清理与挖掘目标相关程度低的数据,将特征字段中的错误值剔除以及将缺省值补齐,将不同记录的数据合并为新的记录值以及对数据进行语法修改形成适用于挖掘技术的统一格式数据等系列工作。(4)模型建立。在“V. 数据挖掘与知识发现”过程中,选择与应用多种不同的挖掘技术,校准挖掘参数,实现最优化挖掘。“控制目标 X_i”下的数据挖掘技术可以将分类与聚类分析、关联规则、统计推断、决策树分析、离散点分析、孤立点检测等技术相结合,用多种挖掘技术检查同一个“控制目标 X_i”的完成程度[12]。选择挖掘技术后,选取少部分数据对目标挖掘技术的实用性与有效性进行验证,并以此为基础,以参数设计、模型设定、模型描述等方式对U模块数据仓库中的数据开展数据挖掘与进行知识发现。(5)解释模型。此过程在模块“W. 模式解释与评价”中完成,中观信息系统审计风险领域专家与数据挖掘工程师需要依据各自的领域知识、数据挖掘成功标准共同解释模块V,审计领域专家从业务角度讨论模型结果,数据挖掘工程师从技术角度验证模型结果。(6)归纳结论。在“Z. 挖掘规律与挖掘路径归纳”中,以W模块为基础,整理上述挖掘实施过程,归纳“控制目标 X_i”下的挖掘规律,探究“控制目标 X_i”下的挖掘流程,整合“控制目标 X_i”($i \in 1 \rightarrow n$)的数据挖掘流程体系,并开发原型系统。

(三) 数据挖掘流程应用举例——“访问控制”下挖掘思路的设计

如前所述,中观信息系统审计包括14个对象,其中“网络管理”对象包含“访问管理”等多个方面。结合COBIT框架下“M_1. 过程监控”与“IT标准-机密性”,“访问管理”可以将“M_1-i. 用户访问网络必须通过授权,拒绝非授权用户的访问”作为其控制目标之一。“M_1-i”数据挖掘的数据来源主要有日志等,本部分截取网络日志对“M_1-i”下数据挖掘流程的设计进行举例分析。

假设某中观信息系统在2011年4月20日18时至22时有如下一段日志记录。

(1)“Sep 20 19:23:06 UNIX login[1015]:FAILED LOGIN 3 FROM(null) FOR wanghua”

(2)“Sep 20 19:51:57 UNIX—zhangli[1016]:LOGIN ON Pts/1 BY zhangli FROM 172.161.11.49”

(3)“Sep 20 20:01:19 UNIX login[1017]:FAILED LOGIN 1 FROM(null) FOR wanghua”

(4)“Sep 20 20:17:23 UNIX—wanyu [1018]:LOGIN ON Pts/2 BY wanyu FROM 172.161.11.342”

(5)“Sep 20 21:33:20 UNIX—wanghua [1019]:LOGIN ON Pts/5 BY wanghua FROM 191.34.25.17”

(6)“Sep 20 21:34:39 UNIX su(pam——unix)[1020]:session opened for user root by wanghua

(uid = 5856)"

… … …

选取上述日志作为数据库,以前文"控制目标 X_i"下数据挖掘的 6 个过程为范本,可以设计"M_1 - i. 用户访问网络必须通过授权,拒绝非授权用户的访问"下的审计证据挖掘流程。该挖掘流程的设计至少包括如下思路:a. 选取"授权用户"作为挖掘的"特征字段",筛选出"非授权用户"的日志数据;b. 以 a 为基础,以"LOGIN ON Pts BY 非授权用户"作为"特征字段"进行挖掘;c. 以 a 为基础,选取"opened … by …"作为"特征字段"实施挖掘。假如日志库中只有 wanghua 为非授权用户,则 a 将会挖出(1)(3)(5)(6),b 会挖出(5),c 将会挖掘出(6)。通过对(5)与(6)嫌疑日志的分析以及"M_1 - i"挖掘流程的建立,IT 审计师就能够得出被审系统的"访问控制"存在固有风险,且 wanghua 已经享有了授权用户权限的结论。

参考文献:

[1]王会金,刘国城. COBIT 及在中观经济主体信息系统审计的应用[J]. 审计研究,2009(1):58 - 62.
[2]阳杰,庄明来,陶黎娟. 基于 COBIT 的会计业务流程控制[J]. 审计与经济研究,2009(2):78 - 86.
[3]张文秀,齐兴利. 基于 COBIT 的信息系统审计框架研究[J]. 南京审计学院学报,2010(5):29 - 34.
[4]谢羽霄,邱晨旭. 基于 COBIT 的电信企业信息技术内部控制研究[J]. 电信科学,2009(7):30 - 35.
[5]黄溶冰,王跃堂. 商业银行信息化进程中审计风险与控制[J]. 经济问题探索,2008(2):134 - 137.
[6]金文,张金城. 基于 COBIT 的信息系统控制管理与审计[J]. 审计研究,2005(4):75 - 79.
[7]陈安,陈宁. 数据挖掘技术与应用[M]. 北京:科学工业出版社,2006.
[8]李也白,唐辉. 基于改进的 PE - tree 的频繁模式挖掘算法[J]. 计算机应用,2011(1):101 - 104.
[9]邓勇,王汝传. 基于网格服务的分布式数据挖掘[J]. 计算机工程与应用,2010(8):6 - 10.
[10]肖伟平,何宏. 基于遗传算法的数据挖掘方法及应用[J]. 湖南科技大学学报,2009(9):82 - 86.
[11]孙强. 信息系统审计[M]. 北京:机械工业出版社,2003.
[12]苏新宁,杨建林. 数据挖掘理论与技术[M]. 北京:科学技术出版社,2003.

[责任编辑:马志娟,刘　茜]

Risk Control System of Meso-Information System Audit: From the Perspective of COBIT Framework of Date Mining Technology

WANG Hui-jin

(Nanjing Audit University, Nanjing 211815, China)

Abstract: At present, a set of risk control system in meso-information system audit is urgently needed in China. First of all, a mature management process is required for the meso economic entities in the control of information system audit risk, and then, state departments also need to have perfect control system as a support in the development of risk prevention standards of information system audit. This paper, based on the description of COBIT framework and data mining theory, firstly, detailed control framework of meso-information system audit risk is constructed in the view of COBIT framework, then, making use of date mining techniques, the data mining path is explored and a mining process created especially as to every detail standard within the framework of the detailed control, and finally, the first two steps are integrated to create a risk control system of information system audit suitable for meso-economic characteristics.

Key Words: meso-information system audit; COBIT framework; date mining; risk control; meso-audit