

基于“业、技、管、审”四融合的公立医院信息系统全生命周期跟踪审计评价体系构建研究*

苏昱霖^①, 邓睿淇^①

摘要 目的: 建立公立医院信息系统全生命周期跟踪审计体系, 规避信息系统高投入、低效益的风险, 提高医院运营的可持续性。方法: 从信息系统全生命周期的角度出发, 与公立医院信息系统特点和审计目标紧密结合, 借助信息技术业务管理体系模型, 以业务审计评价为根本, 以技术审计评价为手段, 再通过管理审计评价进行控制。结果: 构建由4个一级指标, 18个二级指标, 77个三级指标组成的信息系统跟踪审计评价体系。结论: 确保公立医院信息系统建设的适度先进和现阶段最优, 以期为公立医院信息系统跟踪审计工作提供参考。

关键词 公立医院; 信息系统; 跟踪审计; 评价体系

中图分类号 R1-9; F23 **文献标志码** B **文章编号** 1003-0743(2023)10-0075-06

Research on the Construction of Public Hospital Information System Life-Cycle Tracking Audit Evaluation System Based on the Integration of “Industry, Technology, Management and Audit” /Su Yulin, Deng Ruiqi//Chinese Health Economics, 2023,42(10):75-79,84

Abstract Objective: To establish the whole life cycle tracking audit system of public hospital information system, avoid the risk of high investment and low efficiency of information system, and improve the sustainability of hospital operation. **Methods:** From the perspective of the whole life cycle of the information system, it is closely combined with the characteristics of the public hospital information system and the audit objectives. With the help of the information technology business management system model, it takes business audit evaluation as the basis and takes technical audit evaluation as the means, and then controls through management audit evaluation. **Result:** An information system tracking audit evaluation system is built, consisting of 4 first level indicators, 18 second level indicators, and 77 third level indicators. **Conclusion:** It is needed to ensure that the construction of public hospital information system is moderately advanced and optimal at this stage, so as to provide reference for the follow-up audit of public hospital information system.

Keywords public hospital; information system; tracking audit; evaluation system

First author's address Audit Office, Sichuan Cancer Hospital, Chengdu, 610041, China

Corresponding author Deng Ruiqi, E-mail: 1262775513@qq.com

公立医院的高质量发展离不开信息系统的支持, 信息系统自产生以来便始终伴随着各种漏洞与缺陷, 与其他风险相比, 信息系统风险更具破坏性和隐蔽性, 特别是随着信息系统规模扩大、功能的增加和技术的复杂化趋向给医院带来越来越大的风险, 对信息系统审计评价提出更高的要求。公立医院信息化建设一般投资大、周期长, 且系统工程较复杂, 若整个过程缺乏信息系统审计人员的监督, 一旦某一环节出现问题, 就会出现系统成本高、开发周期长、系统功能缺失导致与医院业务管理脱节、内部控制薄弱、缺乏必要的审计线索等问题。此外, 信息系统一旦投入使用, 任何功能的改动成本都异常高昂。因此, 医院内部审计人员必须介入信息系统建设的全过程, 从事后审计转变为全生命周期跟踪审

计, 持续、全面了解系统, 才能有效降低医院所承担的风险, 提高审计效率^[1]。

公立医院信息系统审计评价受限于内部审计人员的非IT专业背景, 审计显得尤为吃力, 目前大部分公立医院对此项审计业务少有开展。基于“业、技、管、审”四融合的公立医院信息系统全生命周期跟踪审计评价体系的构建能有效规范公立医院信息系统跟踪审计评价工作, 同时提高医院运营的可持续性, 最大程度保障医院资产价值。审计评价结果有助于公立医院信息系统从全生命周期及全流程进行监管及规范, 使内部审计目标最终满足公立医院业务管理上的需求。

1 构建思路

1.1 总体思路

公立医院信息系统建设重技术, 轻业务管理, 导致公立医院购买的信息系统与业务管理融合的成功率低, 后期使用效率低, 造成国有资产浪费^[2]。本研究构建的体系运用了《信息技术 业务管理体系》(GB/T37725-2019)的思路和观点, 结合全生命周期理论, 在“业、技、管、审”四融合的环境下, 信息系统审

* 基金项目: 四川省卫生经济学会研究课题(2020SCWJB010)。

①四川省肿瘤医院审计处 成都 610041

作者简介: 苏昱霖(1989—), 女, 硕士学位, 高级审计师, 国际注册内部审计师(CIA), 国际注册风险管理确认专业资格(CRMA); 研究方向: 内部审计、内部控制; E-mail: 449211681@qq.com。

通信作者: 邓睿淇 E-mail: 1262775513@qq.com。

计评价的内容更加丰富。传统信息系统审计评价从一般控制与应用控制出发，更多是关注系统本身。而四融合的公立医院信息系统跟踪审计评价认为信息系统不是一座孤岛，它是将公立医院业务与管理、信息技术与审计评价一体化，要求审计评价与医院业务与管理、信息技术充分融合，审计评价支持公立医院管理决策，站在公立医院的战略角度，判断信息系统是否真正做到有效。

1.2 公立医院信息系统全生命周期阶段划分

全生命周期理论是一个单位对项目建设进行管理的方法论，信息系统的生命周期指系统从启动到消亡所经历的一系列阶段^[9]。公立医院为节约人力成本和时间，信息系统多为直接购买，作为公益性事业单位，信息系统项目在启动前都会由需求科室提出申请，由信息管理委员会评估可行性和必要性。因此，在启动前会多出1个阶段，即项目规划阶段。从项目管理角度考虑，针对公立医院的医院信息系统全生命周期可分为规划、启动、执行和消亡4个时期^[4]，每1个时期又进一步划分成若干个阶段（图1）。

1.3 信息技术业务管理体系

《信息技术 业务管理体系》（GB/T37725-2019）规定了信息系统的业务规划过程、融合转换过程、技术实现过程，主要展现了组织管理、业务活动与信息技术之间的关联关系。

“业务规划过程”是在组织的战略指导下，集中反映业务管理体系中的业务管理规划活动，制定业务总体规划管控与规划策略。业务规划过程的设计和优化应结合组织的实际情况，明确责任、持续改进，管控策略应体现效用、效率、效果及连续性，注重资源权限合理分配，优化业务流程中的审批路径，符合组织对管

理的定位。“融合转换过程”体现业务管理体系从业务管理到技术操作执行的融合与转换过程，即把管理层的业务管理意图转化为具体的操作标准，保证业务统一，真实完整，规范运作。“技术实现过程”集中反映对业务管理中的信息技术支持性活动，利用信息技术实现系统的设计、开发、运维等，并通过对信息技术的管理，保证技术的安全可用、可靠保密，保持信息系统与业务需求一致，推动业务发展，促使效益最大化。

本研究将信息技术业务管理体系的思路融入信息系统全生命周期管理中，二者相辅相成，共同构建业务、技术、管理、审计四融合的信息系统跟踪审计评价体系。

1.4 公立医院信息系统跟踪审计评价体系模型

基于“业、技、管、审”四融合的公立医院信息系统跟踪审计评价体系是以业务审计评价为根本，以技术审计评价为手段，以管理审计评价为控制。业务层面着重从真实性、完整性、符合性、合规性进行评价；技术层面考虑安全性、保密性、可靠性、可用性^[5]；管理层面重点评价效用性、效率性、效果性、连续性^[6]。将业务、技术、管理与审计充分融合，相互作用，共同构成公立医院信息系统审计评价体系，全面评价公立医院信息系统在规划、启动、执行、消亡中暴露的风险点。业务、技术、管理应贯穿于信息系统全生命周期的审计评价中（图2）。

2 公立医院信息系统跟踪审计评价体系构建

2.1 指标选取原则

公立医院的的目标、任务、性质和服务对象的特殊性决定了公立医院信息系统是目前企业级信息系统中最为复杂的一类。公立医院信息系统一般分为3类：一

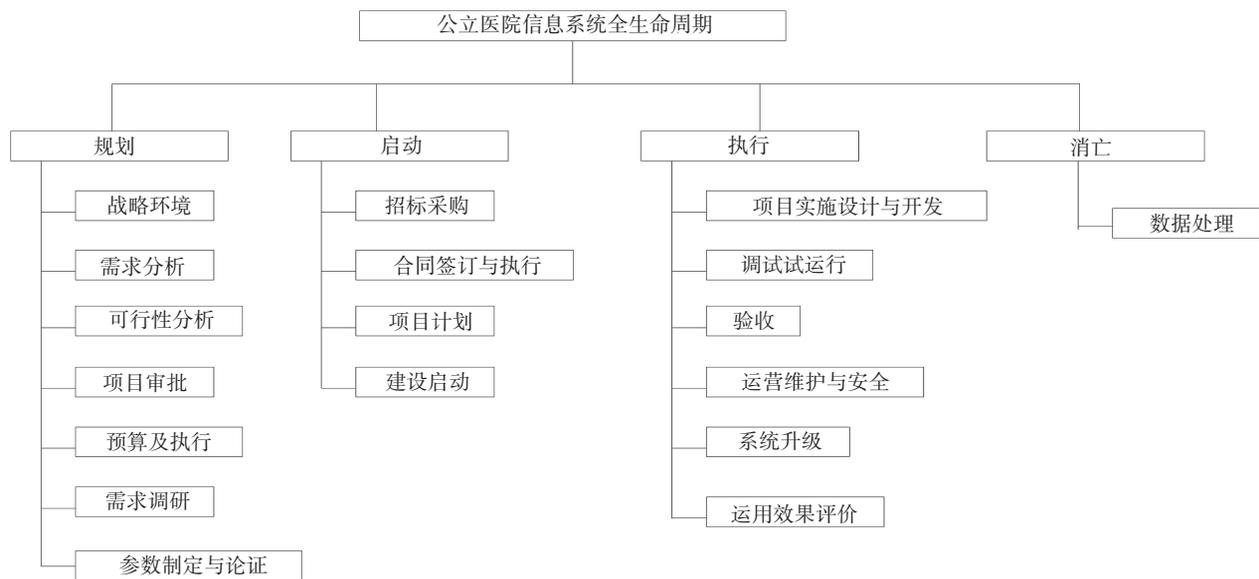


图1 公立医院信息系统全生命周期

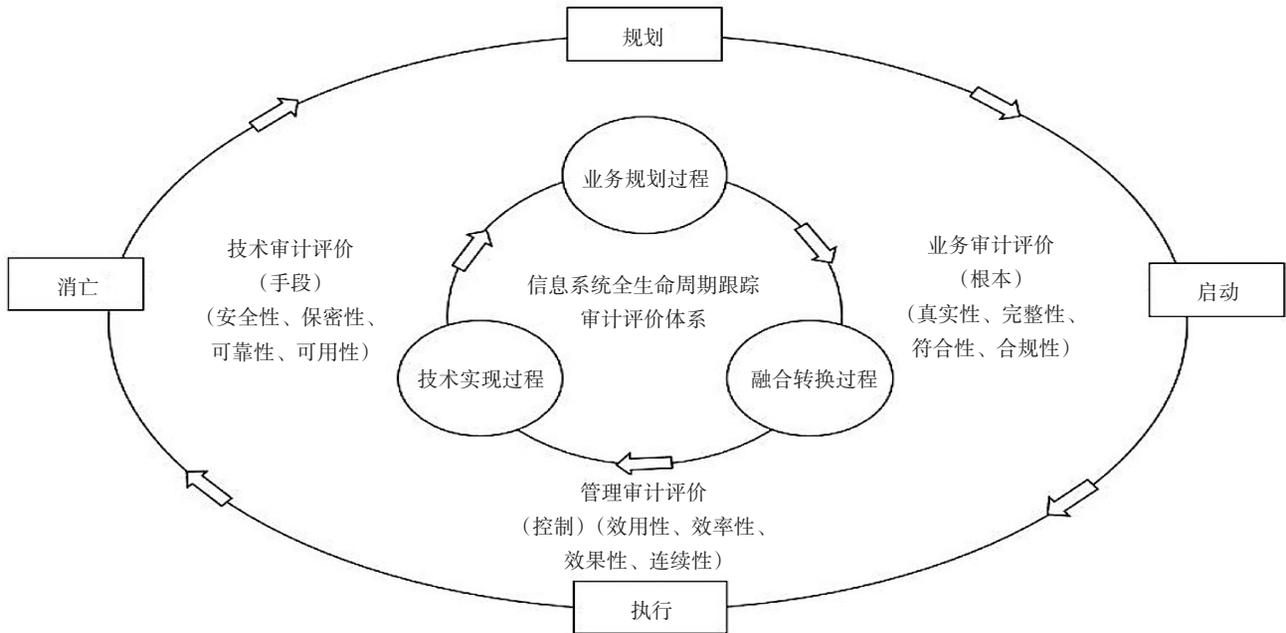


图2 信息系统全生命周期跟踪审计评价体系模型

是满足管理要求的管理信息系统；二是满足医疗要求的医疗信息系统；三是满足以上两种要求的信息服务系统。这些信息系统具有对临床信息和管理信息的高度共享和响应实时性、医疗信息的复杂性与标准化、安全保密性要求高、数据量大、信息共享需求水平高等特点。公立医院兼具政府主导性与公益性，使得在信息系统审计评价时，不应过多考虑其经营的效益。

本研究的指标选取遵循《内部审计基本准则》《第2203号内部审计具体准则——信息系统审计》《审计署关于加强信息系统审计工作指导意见》《审计署关于检查信息系统相关审计事项的指导意见》的相关规定，同时以《COBIT®2019 框架：治理和管理目标》《第3205号内部审计实务指南——信息系统审计》的相关内容作为评价标准，结合全生命周期理论，以及公立医院业务与管理的实际情况，选取针对性强的评价指标，再运用德尔菲法广泛征求公立医院内审部门及社会审计专家意见，按照重要性原则对指标进行“裁剪”，同时兼具科学性与可操作性。

2.2 指标体系构建

基于“业、技、管、审”四融合的公立医院信息

系统全生命周期跟踪审计评价体系由4个一级指标，18个二级指标，77个三级指标构成，详见表1。

体系评价标准层面以信息系统全生命周期的“规划、启动、执行、消亡”4个维度为主线，构建跟踪审计评价指标的总体框架，在此基础上以评价流程为导向，对每个维度的评价指标进行细化，界定指标类型和指标属性：(1) 规划层面以战略环境全面评估为基点，项目审批、预算管理等合规性评估为抓手，重点对需求分析、调研、可行性分析、参数制定与论证等过程结合业务指标、管理指标与技术指标进行评价。侧重从医院管理的政策导向方面进行综合评估，确保信息系统战略与医院战略的一致性，保证系统使用者对系统目标和风险的正确理解，引导对医院信息资源的有效、规范利用。(2) 启动层面评价体系构建主要涵盖招标采购、合同签订与执行、项目计划、建设启动4个阶段，以系统建设前期的招采、合同订立行为全过程以及实施计划与方案层面为评估重点，主要关注流程合规性与符合性，对流程设计与实施不规范引发的法律和经济风险进行评估，进而为系统建设实现杜绝漏洞、风险可控、规范管理探寻路径。(3) 执行层面评价体系构建重点关注信息

表1 基于“业、技、管、审”四融合的公立医院信息系统全生命周期跟踪审计评价体系

评价标准层面	评价流程层面	评价指标层面	指标类型	指标属性
规划	战略环境	信息化质量控制与管理制度、风险应对措施、流程机制是否健全完善	管理指标	效用性
		是否建立了信息管理委员会	管理指标	效用性
		信息管理部的组织架构、人员结构与职责分工、授权审批是否合理	管理指标	效用性
		信息系统目标是否与医院的战略规划一致，满足医院战略需求	业务指标	符合性
		信息系统目标是否与医院信息系统以及管理控制流程相符，具有实用性和操作性	业务指标	符合性
		信息系统战略规划是否得到管理层的许可，是否形成文档	业务指标	合规性

续表 1

评价标准层面	评价流程层面	评价指标层面	指标类型	指标属性
启动	需求分析	是否对系统建设必要性进行充分论证	管理指标	效用性
		是否存在系统规划不合理, 导致重复建设与投资	管理指标	效用性
		是否存在系统需求分析不当, 不符合业务处理和控制需要, 导致开发建设失败或应用价值不高的风险	管理指标	效果性
		是否制定需求变更流程, 对需求变更进行评估跟踪, 防止需求无序增加导致项目成本增加或延期完成风险	管理指标	效用性
	可行性分析	是否从经济、技术、操作、法律、管理等方面进行可行性分析并将可行性报告经业务需求部门负责人签字确认	业务指标	符合性
	项目审批	信息系统投资项目是否经信息系统决策部门批准	业务指标	合规性
		是否存在项目立项未批复即开始实施, 导致项目不合规风险	业务指标	合规性
	预算及执行	预算编制程序是否规范, 是否存在超预算或预算虚高风险	业务指标	合规性
		是否存在提前支付、拖欠支付或超额支付的情况	业务指标	合规性
	需求调研	是否结合医院实际提出需求	业务指标	符合性
	参数制定与论证	参数条款制定是否经过充分论证	管理指标	效用性
		参数条款制定是否具体全面	技术指标	可靠性
	招标采购	招标采购程序是否规范	业务指标	合规性
		招标文件的制定是否全面合理	业务指标	完整性
是否存在化整为零、规避公开招标的行为		业务指标	合规性	
合同签订与执行	是否走合同审签流程	业务指标	合规性	
	合同内容是否完善、切合实际需要, 关键条款是否清晰	业务指标	符合性	
	合同在实施期和运维期是否严格执行	业务指标	符合性	
	在合同执行中发生重大变动时, 是否及时沟通并走变更程序	业务指标	合规性	
项目计划	是否制定切实可行的项目实施计划与实施方案	业务指标	符合性	
建设启动	是否照搬其他医院而未结合本院实际进行建设	业务指标	符合性	
执行	项目实施设计与开发	是否对对外委托开发项目进行有效管理与控制、沟通, 有开发过程中信息管理部门与委托方的协调与沟通记录	管理指标	效用性
		项目开发人员配备是否充足, 关键技术人员是否具有胜任能力	管理指标	效用性
		信息管理部门是否存在未对系统建设进度、质量进行控制导致质量不合格、工期延误的情况	管理指标	效率性
		是否频繁更换或修改系统功能, 未走变更程序或变更程序不合理, 导致法律纠纷或工期延误	业务指标	合规性
		系统开发是否无业务部门人员参与、未定期与业务部门共同审核系统开发建设情况、未及时发现系统不满足业务需要, 导致与业务需求不符的风险	业务指标	符合性
		是否存在离职人员未签订保密协议造成泄密的情况	技术指标	保密性
		是否持续开展信息安全检查工作, 推进安全体系的持续完善	技术指标	安全性
		是否对数据录入的准确性、完整性进行控制	技术指标	可靠性
		是否对数据的修改、删除、校验、入库、共享交换、备份与恢复、转换、整理、计算、汇总等建立有效的管理与约束机制	技术指标	可靠性
		是否对数据的外设、检索、共享、备份与恢复的输出建立有效的管理与约束机制	技术指标	可靠性
	调试试运行	是否对系统测试发现的漏洞缺陷进行管理与跟踪, 保障软件缺陷完整解决	管理指标	连续性
		业务流程中关键环节的相关控制点是否得到有效执行	管理指标	效用性
		是否对信息系统完整性进行检验	业务指标	完整性
		是否对非法数据的容错能力、系统抗干扰能力、突发事件应变能力、系统遭破坏后的恢复能力进行重点测试	技术指标	安全性
	是否对运行人员、业务管理人员、业务操作人员、系统使用人员进行必要的培训	技术指标	可用性的	

续表 1

评价标准层面	评价流程层面	评价指标层面	指标类型	指标属性		
验收		系统实施结果是否未经充分测试即投入使用，程序功能上的缺陷或系统配置上的错误未能及时发现，导致系统运行不稳定或业务功能失效的风险	技术指标	可靠性		
		测试人员是否未依据安全技术标准进行安全测试，发生数据安全事故	技术指标	安全性		
		是否根据项目目标进行规范、按时验收	管理指标	效率性		
		是否存在未达标就通过验收的情况	业务指标	合规性		
		信息系统功能模块是否完整	业务指标	完整性		
		运营维护与安全		运维过程中出现问题，是否无有效应急处理预案，导致系统运行效率低	管理指标	效率性
				系统供应商是否配备有经验的运维人员持续解决使用科室使用过程中遇到的问题	管理指标	连续性
				是否有有效的监控与故障管理措施，监控与故障记录是否完善，监测到异常时是否得到及时处理	管理指标	效用性
				日志管理是否规范，符合相关规定	业务指标	合规性
				是否有专人定期进行系统及数据维护并有巡检维护的记录	技术指标	可靠性
是否按内部控制为系统操作人员设置访问与操作权限	技术指标			安全性		
系统操作人员不相容岗位是否分离	技术指标			安全性		
是否对信息安全进行集中管理且纳入部门工作绩效，实现信息安全管理规范化、体系化建设与全面执行	技术指标			安全性		
是否对机房等重要设施采取防护措施，防止安全隐患	技术指标			安全性		
是否根据业务需要采取有效传输安全控制措施，防止数据泄露	技术指标			安全性		
系统升级		是否对主机访问进行控制，防范黑客入侵或被植入恶意代码，对主机进行违规操作	技术指标	安全性		
		在设计、编码、测试时是否考虑应用系统的安全控制措施	技术指标	安全性		
		是否对数据进行全生命周期的安全管理	技术指标	安全性		
		是否对访问进行控制，避免重要数据被非法访问，导致医院敏感信息泄露	技术指标	安全性		
		是否对安全补丁、漏洞及时升级，对数据备份，对密码和存储介质进行安全防护	技术指标	安全性		
		是否存在系统升级不及时影响业务工作的情况	管理指标	效果性		
		对系统升级变更时，未对历史数据继承和迁移给予足够重视，未进行数据兼容性分析导致历史数据无法使用和继承	技术指标	可用性		
		运用效果评价		系统使用人员满意度	管理指标	效果性
				系统是否出现使用率低的情况	管理指标	效率性
				系统供应商的合同履约率	管理指标	效用性
系统的运用是否真正提高了使用科室工作质量和效率	管理指标			效率性		
与医院其他信息系统是否能很好对接	管理指标			效果性		
是否建立供应商动态考评机制	管理指标			效果性		
是否由于信息化建设缺乏长远和统筹规划，造成不同系统间形成彼此隔离的信息孤岛	管理指标			效用性		
信息化管理制度是否得到有效执行	管理指标			效果性		
功能、性能、易用性与业务需求的符合程度	业务指标			符合性		
医院业务活动对系统依赖程度	业务指标			符合性		
消亡	数据处理	系统业务流程设计合理性	业务指标	符合性		
		与业务管理的相关信息是否均在信息系统中并真实可信	业务指标	真实性		
		是否对数据进行了转移、备份、归档、丢弃、销毁并对软硬件进行密级处理	技术指标	保密性		

系统的设计、开发、建设是否满足业务需求，项目交付与验收能否通过测试和评估，系统变更是否影响当前业务。此外，以系统运行的有效性、可靠性和安全性，用

户使用安全性和效率，系统运维时的应急处理和系统升级的可持续管理为核心对信息系统运行进行多维度评估。
(▶▶下转第 84 页▶▶)

由集团审计部门整体安排、统一调度，与分院区联合开展审计，有效缓解多院区监督管理需求增多与审计资源分散紧缺的矛盾；另一方面大部分异常信息和疑点问题可以直接在平台上进行处理与反馈，减少现场核查频次，避免对业务科室正常工作的干扰，实现审计资源集约高效利用。

3.4 固化数字化审计成果，开展持续评估与改进工作

基于系统数据利用作业经验将审计方法、审计规则转化为数据分析模型并形成审计模型库，成熟一个开发一个，实现数字化审计手段的模型化、通用化、动态化。平台试运行期间通过对预警信息做后评估，发现部分数据需进一步核实确认，通过现场核查结果反推平台模型构建以及规则校验，不断优化审计模型的数据取值空间。

4 小结

本研究以样本医院为例，提出了公立医院数字化审计平台建设应用框架及功能设计思路，因平台处于探索建设阶段，部分审计模型及规则设置合理性有待进一步讨论和确认；平台能否符合预期效果、是否会出现新的问题，还需要长期的探索与研究。

关于未来大数据审计工作的几点思考：一是从国家层面出台一些硬性规定或者刚性要求，比如在医院

等级评审、大型医院巡查、公立医院绩效考核中，把审计信息化建设纳入考核范围、量化考核指标，提升内审高质量发展内生动力，形成长效机制，推进审计信息化建设的持续、有序发展；二是从国家层面进行数字化系统的规划建设，形成一套自上而下、统一规划的审计管理平台供全国医院使用，一方面国家层面可以统揽全局，另一方面地方医院也可以对标找差距、补短板；三是随着紧密型医联体建设发展和信息共享程度的提高，可以建立医联体数据中心，审计平台适时对接并实时抓取数据，审计组可直接在会议室或者专家评审室里进行远程审计。

参 考 文 献

- [1] 葛乌兰. 医院内部审计数字化平台建设探析[J]. 现代经济信息, 2022(33):134-136.
- [2] 张睿, 丁涛, 张欢, 等. 企业内部审计风险预警体系构建——基于大数据背景与霍尔三维结构模型的应用[J]. 中国内部审计, 2022(11):4-11.
- [3] 吴玉清, 刘军燕. 基于信息化手段的医院现代风险导向审计研究[J]. 中国医院管理, 2019,39(4):32-34.
- [4] 祝芳芳, 余平, 操礼庆, 等. 大数据背景下公立医院医疗服务审计模型构建及应用[J]. 中国卫生经济, 2022,41(11):86-90.

[收稿日期: 2023-06-13] (编辑: 彭博)

(◀◀上接第79页◀◀)

医院管理层应当确保系统控制效果、现有控制评估应当体现业务要求，进而运用评价结果及时对系统进行修正。(4) 消亡层面即系统废弃阶段，信息系统进入废弃阶段后，需对其中储存的数据进行转移、备份、归档、销毁并进行密级处理，本阶段侧重评价系统数据处理的保密性，完善信息系统全生命周期闭环管理机制。

3 总结与展望

信息系统生命周期是周而复始进行的，一个系统从规划到消亡会被反复且持续不断地评价，也会不断出现新问题，在审计评价中通过对发现问题的整改完善，利用评价结果建立长效机制^[7]，最终实现PDCA闭环管理。以上指标体系覆盖公立医院信息系统生命周期全过程工作，基本确保不存在重大审计评价盲区而导致的系统性风险。本研究通过将公立医院信息系统建设与应用的全过程置于有效的管理与控制之下，客观、公正、多层次、全方位地对信息系统进行跟踪审计评价，以确保公立医院信息系统建设的适度先进和现阶段最优。

基于“业、技、管、审”四融合的公立医院信息系统全生命周期跟踪审计评价体系作为阶段性研究成

果为公立医院信息系统评价体系构建与实务应用提供理论指引，实务应用层面可根据医院信息系统实际运作情况，借助层次分析等统计学方法予以运用推广，再结合国家政策标准的变化以及公立医院战略发展需求及时更新评价指标，并在实践中不断完善。

参 考 文 献

- [1] 彭源. 浅析信息系统跟踪审计[J]. 中国内部审计, 2010(9):84.
- [2] 金文, 张金城. 基于COBIT的信息系统管理控制与审计的模型构建研究[J]. 审计研究, 2005(4):75-79.
- [3] 陈洁. 基于全生命周期的医院信息化项目管理过程的研究与实现[J]. 中国数字医学, 2016(3):114-115.
- [4] 黄奕宁, 徐莉娅. 基于全生命周期的医院信息系统质量管理[J]. 中国卫生质量管理, 2020(3):81-83.
- [5] 胡俊芬. 基于COBIT框架的软件企业内部控制体系构建[J]. 财会通讯, 2014(5):71-73.
- [6] 陈耿, 李婷婷, 韩志耕. ISACM: 现代信息系统审计模型及其方法体系[J]. 会计之友, 2019(9):125-129.
- [7] 陈杰鹤. 利用外部专家开展医院信息系统投资审计的方法探索[J]. 中国卫生经济, 2018,37(7):85-87.

[收稿日期: 2023-06-18] (编辑: 彭博)