基于COBIT 5.0的国内银行信息系统审计研究与改进

——以拉赫杰银行（Al Rajhi bank）为对比案例

吴静琨

北京工商大学，中国·北京　102488

【摘　要】信息系统审计已经逐渐成为国内外各大银行规范运营与谋求发展的重要工具，为银行内部持续运营、风险管控、评价审核的可靠运行提供保障，极大程度的保证了银行各项信息资产的价值稳定和金融体系的运营稳定。本文通过分析国内银行信息系统审计的现状和相关问题，认为国内各大银行仍未将基于COBIT 5.0的信息系统审计适应于内部运营建设。因此，笔者通过引入世界著名银行拉赫杰银行（Al Rajhi bank），分析该银行基于COBIT 5.0对信息系统审计框架的改进，以及对管理控制目标与应用系统的精简与实施。最后，将从体系建设、审核评价、影响因素确定等方面出发，更多角度的为国内银行信息系统审计进一步应用与提升内部信息系统水平提供思路。

【关键词】信息系统；信息系统审计；COBIT 5.0

Research and Improvement of Domestic Bank Information System Audit Based on COBIT 5.0

—Taking Al Rajhi bank as a comparative case

Wu Jingkun

Beijing Technology and Business University, Beijing 102488, China

[Abstract]Information system auditing has gradually become an important tool for major banks at home and abroad to standardize their operations and seek development. It provides guarantee for the bank¡¯s internal continuous operation, risk management and control, and the reliable operation of evaluation and auditing, and guarantees the bank¡¯s various information to a great extent. The value of assets is stable and the operation of the financial system is stable. This paper analyzes the current situation and related problems of domestic bank information system auditing, and believes that major domestic banks have not yet adapted the information system auditing based on COBIT 5.0 to their internal operation construction. Therefore, by introducing the world-renowned bank Al Rajhi bank, the author analyzes the improvement of the bank's information system audit framework based on COBIT 5.0, as well as the simplification and implementation of management control objectives and application systems. Finally, starting from the aspects of system construction, review and evaluation, and determination of influencing factors, it will provide ideas for the further application of domestic bank information system auditing and the improvement of the level of internal information systems from more perspectives.

[Key words]information system; information system audit; COBIT 5.0

引言

互联网时代早已到来，日新月异的信息技术也已经渗透到各行各业。近几年，国内各大银行对于信息化建设的各项投资逐步加大，从侧面认证了传统管理方法已然不能适应信息化时代公司管理的现状，同时，也证明了信息规范对银行内部稳定运营起到了举足轻重的作用。因此，信息化系统在各大银行应运而生。

信息系统在二十一世纪前便已经引入国内各大银行，但从初时引入至今，银行内部仍时常出现由信息系统故障而引起的重大银行操作失误事件，引起阵阵舆论热议。因此，将审计与信息系统相结合，对降低信息系统各项潜在风险有重要意义。而COBIT 5.0作为ISACA（国际信息系统审计协会）发布的控制框架，能够辅助信息系统评价体系，并且为之提供多维度的规范评价方法，高效率的目标建设与传递，以及为银行对自身信息系统的需求认知提供确定性。

由于COBIT 5.0是国际信息系统审计协会对信息系统审计的总体规范框架，因此并不能完全适应于银行建设。本文选取世界著名银行拉赫杰银行（Al Rajhi bank）为代表，将从COBIT 5.0 的信息系统治理组成与内部业务划分、风险管理模型为角度阐述拉赫杰银行对以COBIT 5.0为基础的信息系统审计改革应用，为国内银行的信息系统建设提出改进建议，完善现有的信息系统审计，并与相关业务进行有效地融合，提高风险管理水平。

1　COBIT 5.0与信息系统审计准则研究

1.1 COBIT 5.0基本框架

COBIT 5.0对信息系统管理分为治理与管理两大部分，其总体以保障银行审计安全、保障银行投资者与用户通明度、优化资源调度、降低多维度风险为目的。并通过满足利益相关者需求、端到端覆盖、采用单一集成框架、启用一种综合方法、区分治理与管理五个重要关键性原则进行规范。

（1）框架内容全面。各国相关机构都曾对信息治理框架提出相关准则，虽然这些准则对信息系统的安全性与可控性都做出一定规范，但相对来说均更侧重某一方面。

（2）五大原则各有特点，配合度高。第一，端到端覆盖，COBIT 5.0的引入为银行信息治理与管理提供了全覆盖的的支持，使得银行内部的治理活动流程清晰。第二，采用单一整合式框架，COBIT 5.0框架是众多风险控制框架与信息系统框架的集成者，并且与该类框架有众多相似之处，可以在使用COBIT 5.0单一整合框架时，进行细节的补充完善。第三，区分治理与管理。COBIT 5.0框架将治理与管理区分开来，既注重了了投资者、客户、公司管理层等利益相关者的需求，又注重了银行本身的内部运行，强调目标、构建、评审等相关事项。两方面相辅相成，有一定的互动性。第四，满足利益相关者的需求。COBIT 5.0框架是银行运用并最终有益于利益相关者的可靠工具，它能够从最终目标逐步向下传递，细化各项举措与公司战略，最终为利益相关者

提供价值。第五，运用整体全面的方法，COBIT 5.0 从七个方面协助银行达到最终目标，七个大面涵盖能力、基础设施、人员水平、行为、企业文化等，提供了一个完整全面的框架，供银行一一规范管理。

（3）普及率较高。COBIT 5.0 作为 ISACA 发布的管理准则，其整体框架已经有接近三十年的发展历史，被世界上大多数国家、大多数行业所接受。不仅如此，20 余年的发展中，COBIT 框架不断进行优化完善，已经包含 IT 审计、控制、管理、治理多个方面，被 170 多个国家的各行各业进行适应性调整，已经具有极高的普及率，使用端规模庞大，借鉴经验充足。

2 国内信息审计准则的应用

2.1 国内银行信息审计准则的应用现状

（1）信息系统审计的审计宽度。目前，国内银行的信息系统审计主要包含对数据文件的审计、对内部控制的审计、对系统开放的审计与对应用程序的审计等，将大部分信息系统审计重点放在运行与维护两大方面，对安全性和运营性做好把关。

（2）信息系统审计的审计流程。与传统的审计相比，信息系统审计主要包括审计计划、审前检查、审计实施、审计报告四个阶段，总体包含完整，但国内银行更偏重安全性和合规性的检查，忽视了创新性和效益型的结果。因此，大多数银行内部只谋求片段式的效益，并没有将信息系统审计彻底地运用于整个内部治理与管理。

（3）信息系统的审计方法。国内银行在进行系统审计时，主要采用实地调查、数据测试、利益相关者反馈等方式。实地进行现场检查，这主要是对控制链中数据的输入与处理，不同业务之间的协办进行实地勘察核定。

2.2 国内银行信息审计准则的存在问题

（1）信息系统审计的审计宽度。目前，国内银行的信息系统审计主要包含对数据文件的审计、对内部控制的审计、对系统开放的审计与对应用程序的审计等，将大部分信息系统审计重点放在运行与维护两大方面，对安全性和运营性做好把关。

（2）信息系统审计的审计流程。与传统的审计相比，信息系统审计主要包括审计计划、审前检查、审计实施、审计报告四个阶段，总体包含完整，但国内银行更偏重安全性和合规性的检查，忽视了创新性和效益型的结果。因此，大多数银行内部只谋求片段式的效益，并没有将信息系统审计彻底地运用于整个内部治理与管理。

(3)信息系统审计方法单一。部分银行缺少必要的技术支持，可使用的软件和计算机审计系统较少，尤其在面对审计系统运行环境变化、业务多角度处理监督的情况时，技术的落后性和缺失性大大降低了审计的效率和质量。同时，当银行采用信息审计系统时，需要及时更新数据保留技术，确保审计证据完整性，进而保证审计质量，提高审计人员的主动性。

(4)信息系统审计业务定义模糊。在信息系统审计中，一般银行主要涉及治理、风险管控、合规化管理以及政策实施这四个主要的方面，但这四个方面内容定义模糊，业务之间责任推脱现象严重，相关工作部门小组形同虚设，降低了预期工作效率，无端消耗内部资源。

(5)信息系统审计专业人员缺失。尽管各大银行越来越重视信息系统审计方面的人才，但该类人才仍相对较少。

3 COBIT 5.0 与信息系统审计准则在拉赫杰银行（Al Rajhi bank）应用与创新

3.1 拉赫杰银行（Al Rajhi bank）简介

拉赫杰银行（Al Rajhi bank）银行成立于 1957 年，是世界上最大的伊斯兰银行之一，总资产为 2880 亿里亚尔（768 亿美元），实收资本为 43 亿美元，员工人数超过 8400 名。凭借 60 多年的银行和贸易活动经验，Al Rajhi 名下的各个独立机构于 1978 年合并为旗下的 Al Rajhi Trading and Exchange Corporation。1988 年，该银行成立为沙特控股公司。目前，拉赫杰银行已经跻身世界百强银行名列。

3.2 拉赫杰银行（Al Rajhi bank）信息系统审计的应用特点

（1）建立管理层支持的目标传递框架。为获得高级管理层的支持，也为了公司目标传递的有效性，拉赫杰银行高层确定银行痛点与银行业务目标，其中，业务目标需要满足合规性要求与监管要求，并且能够缩小审计差距，将信息系统审计与公司治理相结合。

（2）建立良好的风险管理模型。拉赫杰银行制作了一个风险管理模型（图 3）。该模型以 COBIT 为基础，包括了风险评估、风险管理、风险反馈以及整体更新，可以满足银行内部的信息系统的性能和合规性要求。其中，风险管理包括判断风险偏好与承受能力、结合银行汇率以及认知风险文化等内容；风险评估包括风险描述、风险类别的判定以及对不同业务的影响定义；风险反馈包括对关键风险指标的定义等；整体更新包括信息系统审计技术的更新、建立最新的监控与指标评级。同时，这四部分可以达成一个循环整体，避免侧重某一部分而出现的管理漏洞。

4 国内银行基于拉赫杰银行（Al Rajhi bank）信息系统审计准则的改进

(1)拓宽信息系统审计范围。信息系统审计不仅应该贯穿业务开发、实施，最后分析反馈的整个过程，更应该对能够影响业务的全部资源与活动进行治理控制。将多条业务线互相的影响力进行交叉式分析处理，建立相应的影响判断标准，对所涉及到的人员、流程合规性、安全性以及最终的效益进行系统评判。

(2)完善信息系统审计流程。首先，银行管理层明确推动信息系统审计可持续性建设的影响因素，明确需要以政策与原则为中心，以此为基础建立审计流程、审计组织结构以及企业文化与道德准则，不仅如此，还要依据该基础获取相关的信息，进行基础信息与应用程序建设，不断提高专业审计人员比例与技能水平（如图 5）。其次，着重风险控制领域的控制流程建设，建立风险发现－风险评估－风险治理－风险反馈的风险循环管理系统，并且将提高技术能力始终贯穿其中。

(3)明确信息系统审计各业务模块的内容组成。细化信息系统审计不同业务的详细内容，重点建立好治理、风险管控、合规化管理、政策实施四大板块的体系细化建设，避免业务重叠导致的责任推脱。不仅如此，细化内容的同时要做到责任到人的分工，各部门明确员工工作，各司其职，提高审计效率。

(4)引进更多信息系统审计人才与审计技术。为了使各个模型框架能够有效地加以实践，国内银行需要重视信息系统审计人才的引进与培养，以及专业审计技术的探索和升级。信息系统审计结合了计算机和审计的专业知识，需要高度技术性与专业性兼具的领域人才。

因此，国内银行首先要对银行的内部审计部门进行信息系统审计的理论与技能培训，提高了解与精通信息系统审计员工的比例。其次，需要对计算机等科技部门进行选择性培训，提高科技部门对于信息系统审计的知晓度，提高未来双方合作效率。最后，积极引进外部人才，重视来自第三方的人才或者合作培养机遇。

参考文献：

[1] 杨佩毅.基于COBIT5.0的银行信息系统审计评价体系构建[J].财会通讯,2021(23):138-141.DOI:10.16144/j.cnki.issn1002-8072.2021.23.027.

[2] 靳少华.基于COBIT5.0的银行信息系统审计优化分析——以上海农商银行为例[J].财会通讯,2019(13):106-109.DOI:10.16144/j.cnki.issn1002-8072.2019.13.024.

[3] 黄力.基于COBIT视角的商业银行信息系统审计研究[J].金融纵横,2019(06):41-49.