DOI:10.19641/j.cnki.42-1290/f.2018.19.016

基于COBIT 5建立财务共享服务中心风险管理机制

刘 霞(副教授), 任驿佳

【摘要】首先通过梳理相关文献,提炼财务共享服务中心风险因子,建立基于COBIT 5的财务共享服务中心风险管理模型;然后两轮使用德尔菲专家问卷,收集专家意见,对该模型予以完善;最终建立财务共享服务中心风险管理机制,包括4个IT管理层面、52项风险因子和130项控制措施。同时,采用案例研究法,通过结构化访谈的方式,对案例公司的副总经理和IT管理部负责人等进行访谈,验证所构建的风险管理机制的有效性。研究结果表明,基于COBIT 5的财务共享服务中心风险管理机制能协助企业通过风险识别、评价、应对、监督与修正完成整个风险管理过程,并快速找出潜在的风险因子,进而实施有效的控制措施,是一个便利、有效的风险管理工具。

【关键词】COBIT 5; 财务共享服务中心; 风险管理机制; 风险因子

【中图分类号】F275 【文献标识码】A 【文章编号】1004-0994(2018)19-0099-15

一、引言

2018年李克强总理在政府工作报告中7次提及“互联网+”信息技术已广泛融入企业管理与运营中,是我国经济转型升级的强劲动力。在这一背景下,对信息技术的投资已成为企业提升竞争力不可或缺的方式,其中财务共享服务中心(Financial Shared Service Center,FSSC)是当前企业最重要的IT投资方式之一。2015年安永华明会计师事务所调查显示,已建立财务共享服务中心的企业中,五年前建立的占比22%,近五年内建立的占比78%,说明财务共享服务中心在我国的发展速度惊人。如何控制财务共享服务中心的风险,在时间、成本、质量等方面实现组织目标,是项目团队与高管层面临的最大挑战。本文的研究目的在于针对财务共享服务中心面临的风险,建立风险管理机制,从而协助企业构建全面的信息安全系统。

Van Grembergen等[1]指出,信息治理可视为公司治理的一部分,是通过建立一套合理的机制,规范组织信息流程与管理框架,协助企业达到信息战略整合与提升价值等目的。为了处理更加深入和广泛的信息技术问题,国际信息系统审计与控制协会(ISACA)于2012年发布了《信息及相关技术控制目标》(Control Objectives for Information and Related Technology)第五版(COBIT 5)。COBIT 5能够确保组织的政策、计划、程序和结构设计实现业务目标,并防止、检查或改正非预期的事件[2],也是企业进行IT风险管理的框架[3]。COBIT 5已成为美国网络安全新框架的核心[4],是国际上公认的最先进、最权威的安全与信息技术管理和控制标准[5]。目前,我国对COBIT的研究以借鉴为主[6],对于COBIT理论应用于信息系统的研究不够深入,尚未有一套完整的信息系统控制规范。因此,本文基于COBIT 5,分析和讨论财务共享服务中心的风险管理系统,识别和

【基金项目】国家社会科学基金后期资助项目(项目编号:17FJY015); 河北省审计厅重点课题(项目编号:201811)

评估风险因子，探讨可供管理层选择的风险应对策略，以帮助企业建立与实施系统、完善的风险管理机制。

本文的贡献在于：首先，对COBIT 5进行了深入研究，将COBIT 5的条款从文字介绍落实到风险管理流程，真正落实到实处，为我国企业信息系统的实施积累经验。其次，扩展了财务共享服务中心的研究范围，目前对财务共享服务中心的研究多集中在概念探讨和现状分析上，本文通过构建财务共享服务中心风险管理框架，分析财务共享服务中心从上线到日常运作的整个过程，辨别和管理影响其上线和运作的风险因子。最后，扩展了风险管理研究范围，当前已有研究主要是针对基于COBIT 5的会计控制系统，研究范围集中于日常会计核算和监督，而本文研究范围从会计控制扩展到风险管理，拓展了风险管理中信息技术的运用范围。

二、文献综述

（一）风险管理程序

美国反虚假财务报告全国委员会的发起组织委员会（COSO）在2014年发布了《企业风险管理整合框架》（COSO-ERM），并于2017年进行了修订。修订后的COSO-ERM将“风险”定义为事项发生并影响战略和业务目标实现的可能性。所有组织中都存在风险，风险管理的最大挑战是将风险控制在组织偏好的范围之内。近几年许多风险管理机制应运而生，如PMI 2001、SAFE Methodology、Risk Diagnosing Methodology，这些都是经典的循环性风险管理机制[7]。财务共享服务中心的风险管理程序可总结为风险识别、风险评估、风险应对、监督与修正。

在财务共享服务中心导入前的选择、导入后的运作和管控的整个过程中，存在的风险包括：系统选择不当、项目团队能力不足、高管层参与度不高、主要使用者参与度低、缺乏训练与指导、不当的企业流程再造、缺乏管理性的指引、无效的项目管理技术、不当的变革管理、缺乏咨询服务、系统供货商的稳定性不佳与战略规划不合理。财务共享服务中心串联整个企业功能，疏于风险管理，很可能会导致企业巨额亏损。因此，财务共享服务中心的风险管理是保证整个企业顺利营运的关键要素之一。

（二）风险管理标准与规范

当前与风险管理相关的标准及规范主要包括：COSO-ERM、《风险管理——原则与实施指导准则》（ISO/IEC 31000）、《信息技术——安全技术——信息安全管理体系——要求》（ISO/IEC 27001）与《信息技术——安全技术——信息安全风险管理》（ISO/IEC 27005）和COBIT 5。COSO-ERM是一个关于风险管理的高层级的概念框架，主要用于组织治理层面，对于IT控制目标和相关活动没有详细的标准。COBIT 5弥补了这一缺陷，其中不但包括组织治理、业务流程等，还列示了IT管理四大领域的详细流程[3]。ISO/IEC 27001与ISO/IEC 27005强调IT管理的具体内容，对IT治理没有涉及。ISO/IEC 31000虽然制定了IT治理的流程，但在IT管理方面仅侧重于调整、规划与组织流程。综上所述，COSO-ERM的原则性较高，COBIT 5不但弥补了COSO-ERM所欠缺的详细流程，还补充和强化了ISO/IEC系列标准的内容。

（三）IT控制与IT治理

企业应建立较为健全的IT内部控制，以防止舞弊、检查错误，降低企业IT风险及其未来可能造成的损失。采用IT技术可以提升企业内部控制质量[8]，IT内部控制框架与标准可以帮助企业适应环境的变化[9]。COSO在2013年更新了内部控制整合框架，其中一项重要原则便是“针对信息技术，组织应选择并执行一般控制活动以支持其目标的实现”。COBIT是一个国际公认的在IT管理和控制方面的权威标准，明确了为实现企业控制目标，IT程序如何传递信息[10][11]。管理层可以运用COBIT框架进行财务报表审计，以评估其IT内部控制的有效性[12]。因此本文认为，通过IT控制能够实现财务共享服务中心风险管理的目的。

IT治理是通过开发和维护一个有效的IT控制与责任机制管理绩效和风险，确保信息系统的实施战略与企业战略得以衔接，实现企业价值最大化。在IT治理与公司治理同时有效运作的情况下可以强化企业管理者的责任[13]。Bin-Abbas等[14]提出了50项IT治理的控制要素，帮助组织发现IT治理的优势和弱点，找到未来治理的发展方向。IT治理研究所（ITGI）指出，COBIT是唯一能够提供IT治理的管理框架，能够支持IT目标的实现，确保IT定位准确，提高IT效率效果。ISACA认为COBIT是以IT程序、IT领域、信息准则和IT资源为基础的流程控制理论。COBIT已成为组织执行IT控制的重要参考框架[12]。因此本文认为，基于COBIT建立财务共享服务中心风险管理机制不但可行，而且对于探讨适

合我国企业的IT控制具有重要意义。

三、研究设计与方法

首先，通过梳理文献，整理归纳出财务共享服务中心风险管理因子，构建基于COBIT 5的财务共享服务中心风险管理初步模型。本文整理的文献主要包括：Jan等[15]、Knol等[16]、Huang等[17]、Marijin等[18]、Martin[19]、Owens[20]、Spears等[21]、何瑛等[22]、张瑞君等[23]以及王光远等[24]。通过对这些文献进行整理，提炼出53项财务共享服务中心风险管理因子。

其次，采用德尔菲专家问卷法检验由文献归纳出的财务共享服务中心风险管理机制是否合理，并取得专家们的一致意见。德尔菲专家问卷调查法是根据专家的专业知识、经验及意见，经由多回合的问卷发放与反馈，获取专家对某一议题的共识的一种研究方法[25][26]。本文聘请了14位从事财务共享服务中心风险管理理论研究的专家和实务工作者，经过以下六个步骤获取专家意见：①成立专家小组；②设计问卷；③发放问卷给专家小组；④针对专家问卷进行分析归纳；⑤若各问项未满足一致性，则重新发放问卷；⑥总结与报告。

最后，采用案例研究法确认所构建财务共享服务中心风险管理机制的有效性。本文以某公司为研究对象，对其总经理、副总经理、信息部主管（CIO）、财务共享服务中心负责人或相关主管、负责执行财务共享服务中心的项目成员进行深度访谈。通过在案例企业现场收集企业实际运作的数据，并辅之以企业所在行业相关的研究报告、数据等资料，进行分析和整理，归纳总结出相关研究结论。

四、构建财务共享服务中心风险管理机制

（一）确认财务共享服务中心的风险管理因子

COBIT 5将IT管理领域分为四个层面：①协调、计划与组织（APO），包括13项控制流程；②建立、获取与实施（BAI），包括10项控制流程；③交付、服务与支持（DSS），包括6项控制流程；④监督、评估与评价（MEA），包括3项控制流程，具体如表1所示。根据这四个层面的特点，将53项风险因子进行分类。下面以“安全措施的效果不佳”风险因子为例进行分析：

第一步，“安全措施的效果不佳”这一风险因子符合APO层面“拟定信息环境框架”的内涵，因此，将该风险因子划分为APO层面，并进行编号“Risk_APO.1安全措施的效果不佳”。

表1　COBIT 5中IT管理领域四个层面的控制流程

层面	控制流程
APO	Pro_APO01界定与管理IT管理标准
	Pro_APO02界定管理战略
	Pro_APO03管理企业框架
	Pro_APO04管理创新
	Pro_APO05管理投资组合
	Pro_APO06管理预算与成本
	Pro_APO07管理人力资源
	Pro_APO08管理关系
	Pro_APO09管理服务合约
	Pro_APO10管理供应链
	Pro_APO11管理质量
	Pro_APO12管理风险
	Pro_APO13管理安全
BAI	Pro_BAI01管理计划与项目
	Pro_BAI02管理需求定义
	Pro_BAI03管理解决方案和计划组织
	Pro_BAI04管理可用性和能力
	Pro_BAI05管理组织变革
	Pro_BAI06变更管理
	Pro_BAI07管理变更的验收与过程
	Pro_BAI08管理知识
	Pro_BAI09管理资产
	Pro_BAI10管理组态设定
DSS	Pro_DSS01管理服务水平
	Pro_DSS02管理第三方服务
	Pro_DSS03管理问题
	Pro_DSS04管理持续性
	Pro_DSS05确保系统安全
	Pro_DSS06确认企业流程控制
MEA	Pro_MEA01监督、评估与评价资产绩效
	Pro_MEA02监督、评估与评价系统内部控制
	Pro_MEA03监督、评估与评价外部规定的遵循

第二步，分析风险因子“安全措施的效果不佳”包括在哪些流程中。专家们针对该风险因子进行讨论，认为涵盖风险因子Risk_APO.1的流程包括“Pro_APO01界定与管理IT管理标准”和“Pro_DSS05确保系统安全”。

第三步，COBIT 5中为上述四个层面的32项控制流程确定了195个控制措施，如在Pro_APO01流程中，对应控制措施有8个：①定义组织结构；②建

立角色和责任；③维护管理系统的实现；④沟通管理的目标和方向；⑤优化IT运作的位置；⑥界定信息（数据）和系统的所有权；⑦持续改进管理的过程；⑧持续遵守政策和程序。与Risk_APO.1相关的控制流程为Pro_APO01、Pro_DSS05，专家们讨论认为相应的控制措施为“持续遵守政策和程序”（对应流程为Pro_APO01），“管理网络连接的安全性”和“管理端点安全性”（对应流程为Pro_DSS05）。据此，本文将这三项控制措施分别编号为“Obj_APO.1.1 持续遵守政策和程序”、“Obj_APO.1.2 管理网络连接的安全性”和“Obj_APO.1.3 管理端点安全性”。

第四步，根据所确定的控制流程与控制措施，参考COBIT 5中列示的26个角色和职能，针对组织内角色与职能给予适当的责任分配。

重复以上步骤，找出其余52项风险因子对应的控制流程、控制措施，并明确对应的角色和职能，最终建立基于COBIT 5的财务共享服务中心风险管理机制初步模型。该模型在APO层面包含20个风险因子（如表2所示）、BAI层面包含18个风险因子（如表3所示）、DSS层面包含9个风险因子（如表4所示）、MEA层面包含6个风险因子（如表5所示），共53个风险因子，对应的具体控制措施为136项。

（二）采用德尔菲法修正研究模型

本研究在建立风险管理机制初步模型后，通过发放德尔菲问卷的方式，取得理论界与实务界专家的意见与共识，并进行模型修正。德尔菲法能够通过多回合的问卷调查整理出一致的意见，且其匿名性可以克服面对面讨论或开会的局限性，让专家们在互不影响的状况下提出合适的意见。

德尔菲法要求进行反复询问，直至专家们达成共识为止，目的是通过专家们的不断讨论，取得较为完善的解决方案。本文运用了两轮德尔菲专家问卷，第一轮是由专家来决定问项归类是否正确且适合作为财务共享服务中心的风险因子，第二轮是针对第一轮中专家意见分歧部分达成共识，再次确认所构建的财务共享服务中心风险管理机制。两轮问卷均以电子邮件的方式发放和回收，问卷回收后采用CVR值检验内容效度[27]，采用四分位差检验专家意见离散程度[28]。

专家小组成员既包括财务共享服务中心领域和风险管理领域的咨询顾问，也包括高校中从事财务共享服务中心和风险管理研究的学者。专家小组的成员为15人左右最佳[25]，本文选取14名专家，其中在企业及政府信息技术相关部门任职的有6人，在会计师事务所或管理咨询公司任职的有6人，在高校任职的有2人。这14名专家的任职时间均值为11年。

1. *第一轮问卷*。第一轮问卷的实施自2017年4月8日开始，5月3日完成所有问卷的收回。问卷设计以逻辑判断为主，并留有空白处使专家能充分表达意见。第一轮问卷结果的检验分为三步完成：

①检验问卷内容的信度和效度，根据问卷填答结果计算CVR值。根据Lawshe[27]的研究，当调研人数为14人时，CVR的最小值为0.51。结果显示，除“Risk_APO.3故意的行为”CVR值小于0.51之外，其余风险因子的CVR值均大于0.51。说明专家对财务共享服务中心环境下的风险因子归类至COBIT 5中IT领域管理四个层面的恰当程度表示高度认同。

②确认所选项目是否适合作为财务共享服务中心的风险因子，四分位差大于0.6或标准差大于1，则表示未达到一致性[28]。结果显示，四分位差大于0.6的控制措施包括Obj_APO.3.2、Obj_APO.3.3、Obj_APO.4.2、Obj_APO.10.1、Obj_APO.10.2、Obj_APO.13.1、Obj_APO.15.1、Obj_BAI.2.1、Obj_BAI.6.2、Obj_BAI.7.2、Obj_BAI.11.3、Obj_BAI.14.1、Obj_DSS.3.2，标准差大于1的控制措施包括Obj_APO.10.2、Obj_APO.12.2、Obj_APO.15.1、Obj_APO.15.2、Obj_APO.19.2、Obj_DSS.4.1、Obj_MEA.1.1，共计18项控制措施未达到一致性。这18项控制措施需要在第二轮问卷中进一步讨论。

③请专家在空白处填写意见，这些意见也将在第二轮问卷中进行讨论。

2. *第二轮问卷*。第二轮共发出14份问卷，全部收回。根据专家意见对风险因子进行了修正，修正结果详见表2～表5。针对在第一轮中未达到内容效度的项目“Risk_APO.3 故意的行为”，第二轮专家意见一致认为其不适合作为风险因子，予以删除。第二轮结果显示，修正后的风险因子“操作系统的瑕疵影响财务共享服务中心系统运作”的CVR值为0.43，低于最低标准，说明其不适合作为风险因子，予以删除。最终剩余52项风险因子，且有些风险因子进行了重分类，如：Risk_APO.17重分类至BAI层面，Risk_BAI.2、Risk_BAI.9、Risk_BAI.12、Risk_DSS.2、Risk_DSS.3均重分类至APO层面。

在第二轮德尔菲问卷中针对风险因子所对应的

表 2　　风险管理机制模型——APO 层面

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_APO.1 安全措施的效果不佳	0.86	Pro_APO01	Obj_APO.1.1 持续遵守政策和程序	0.5	0.75	4.31	财务共享服务中心系统信息安全保护措施不佳		0.5	0.51	4.38
		Pro_DSS05	Obj_APO.1.2 管理网络连接的安全性	0.5	0.60	4.23			0.5	0.83	4.23
			Obj_APO.1.3 管理端点安全性	0.5	0.73	4.23			0.5	0.65	4.38
Risk_APO.2 经授权的使用者误用	1.00	Pro_APO01	Obj_APO.2.1 界定数据和系统的所有权	0.5	0.73	4.29					
		Pro_DSS05	Obj_APO.2.2 监督基础设施及与安全相关的事件	0.5	0.80	4.21					
		Pro_DSS06	Obj_APO.2.3 管理角色、职责,以及存取权限和级别的权限	0.5	0.52	4.50					
Risk_APO.3 故意的行为	0.43	Pro_APO13	Obj_APO.3.1 监督和审查	0.375	0.88	4.10	预计删除风险因子				
		Pro_BAI07	Obj_APO.3.2 建立一个测试环境	0.875	0.88	4.10					
		Pro_DSS05	Obj_APO.3.3 监督基础设施及与安全相关的事件	0.875	0.88	3.90					
		Pro_MEA01	Obj_APO.3.4 确定一个监督的方法	0.375	0.74	3.90					
Risk_APO.4 职责无分工	0.86	Pro_APO12	Obj_APO.4.1 简述风险	0.5	0.75	4.31	角色职权未适当分工,造成权力过度集中		0	0.58	4.00
		Pro_MEA02	Obj_APO.4.2 执行控制的自我评估	1	0.82	4.00			0.5	0.69	4.15
Risk_APO.5 难以整合各个部门	1.00	Pro_APO08	Obj_APO.5.1 协调和沟通	0.5	0.65	4.43					
Risk_APO.6 与旧系统整合的挑战	1.00	Pro_APO01	Obj_APO.6.1 维护管理系统的实施	0.5	0.50	4.36					
		Pro_BAI05	Obj_APO.6.2 形成有效的执行团队	0.5	0.63	4.36					
		Pro_DSS01	Obj_APO.6.3 管理环境	0.375	0.66	4.14					
Risk_APO.7 缺乏充分的训练计划	1.00	Pro_APO07	Obj_APO.7.1 确定关键的IT人员	0.375	0.77	4.14					
		Pro_BAI08	Obj_APO.7.2 组织信息转化为知识	0.5	0.77	4.14					
Risk_APO.8 技术人员的效能问题	0.86	Pro_APO07	Obj_APO.8.1 保持足够且适当的人力资源	0.5	0.60	4.23					
			Obj_APO.8.2 组织信息转化为知识	0.5	0.60	4.23					
			Obj_APO.8.3 评估职员的工作绩效	0.5	0.51	3.62					
Risk_APO.9 使用者涉入不足	1.00	Pro_APO08	Obj_APO.9.1 协调和沟通	0.5	0.76	4.50					

续表 2

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_APO.9 使用者涉入不足	1.00	Pro_APO09	Obj_APO.9.2 确定 IT 服务	0	0.62	3.93					
		Pro_BAI02	Obj_APO.9.3 界定和维护业务功能和技术要求	0	0.62	4.07					
			Obj_APO.9.4 进行有效性研究	0.375	0.66	4.14					
Risk_APO.10 系统不符合运营流程	0.86	Pro_APO01	Obj_APO.10.1 界定组织结构	1	0.86	4.08	财务共享服务中心系统因组织结构的问题而不符合运营流程		0	0.64	3.92
		Pro_APO02	Obj_APO.10.2 了解企业发展方向	1	1.24	3.77			1	0.86	3.92
		Pro_BAI02	Obj_APO.10.3 界定和维护业务功能和技术要求	0	0.71	4.00			0.5	0.69	3.85
Risk_APO.11 不适合的技术任务	0.71	Pro_APO02	Obj_APO.11.1 沟通 IT 战略及方向	0.125	0.67	3.92	计划极端评定不适当的科技技术任务，造成财务共享服务中心运作错误		0	0.55	3.85
		Pro_APO03	Obj_APO.11.2 选择机会和解决方案	0.125	0.67	3.92			0	0.64	3.92
		Pro_APO04	Obj_APO.11.3 监督和审视技术环节	0	0.79	3.92			0.5	0.76	4.08
		Pro_BAI02	Obj_APO.11.4 评估潜在的新兴技术和创新理念	0.125	0.83	3.83			0.5	0.83	3.92
			Obj_APO.11.5 界定和维护业务功能和技术要求	0.125	0.58	3.83			0.5	0.65	3.62
Risk_APO.12 缺少适当方法	0.86	Pro_APO02	Obj_APO.12.1 界定战略性计划和路线图	0.5	0.95	3.69	未有与财务共享服务中心配合的方法		0.5	0.78	3.54
		Pro_BAI08	Obj_APO.12.2 培育并促进知识共享的文化	0.5	1.04	3.62			0.5	0.80	3.85
Risk_APO.13 没有适当规划	0.71	Pro_APO02	Obj_APO.13.1 了解企业发展方向	1	1.00	3.92	未寻求咨询公司进行适当的规划		0	0.58	4.00
		Pro_BAI01	Obj_APO.13.2 监督并控制项目	0.125	0.67	3.92			0.5	0.69	4.15
Risk_APO.14 人力资源政策未改变	1.00	Pro_APO07	Obj_APO.14.1 计划和追踪 IT 企业人力资源的使用	0.5	0.70	4.21					
Risk_APO.15 公司现有文化问题	0.86	Pro_APO03	Obj_APO.15.1 界定架构	1	1.19	3.62	管理层提出的可能影响系统运作的公司文化问题		0.5	0.69	3.85
		Pro_APO04	Obj_APO.15.2 建立一个有利于创新的环境	0.5	1.12	3.62			1	0.82	4.00
Risk_APO.16 组织现有结构问题	1.00	Pro_APO01 Pro_APO03	Obj_APO.16.1 界定组织结构	0.5	0.85	3.50					
		Pro_BAI05	Obj_APO.16.2 开发企业架构的愿景	0.5	0.84	3.64					

续表 2

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_APO.17 供应商问题	0.71	Pro_APO08	Obj_APO.17.1 管理业务关系	0.5	0.89	3.67	系统供应商端口在系统的取得、开发和维护上的问题	BAI	0.5	0.77	3.62
		Pro_APO10	Obj_APO.17.2 识别和评估供应商的关系和合约	0.125	0.85	4.00			0.5	0.60	4.23
Risk_APO.18 团队组成不稳定	0.86	Pro_APO03	Obj_APO.18.1 定义所实施的组织架构	0.5	0.77	3.38					
		Pro_BAI05	Obj_APO.18.2 提供企业基础架构服务	0.5	0.52	3.54					
			Obj_APO.18.3 保持的变化	0	0.64	3.92					
Risk_APO.19 资源不足	0.71	Pro_APO06	Obj_APO.19.1 优先考虑资源分配	0.5	0.52	4.50	财务共享服务中心系统所需资源不足		0.625	0.79	4.08
		Pro_BAI09	Obj_APO.19.2 识别和记录当前的资产	0.5	1.07	3.33			0.625	0.79	3.92
Risk_APO.20 人员任用不适当	0.86	Pro_APO07	Obj_APO.20.1 保持足够和适当的人力资源	0.5	0.63	4.31	人力资源政策未改变而导致人员任用错误		0.5	0.76	4.08

表 3　　风险管理机制模型——BAI层面

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_BAI.1 输入错误或窜改资料	0.86	Pro_BAI03	Obj_BAI.1.1 构建解决方案	0.5	0.51	4.62	输入错误或窜改资料(可恢复改正)		0.5	0.65	4.33
		Pro_BAI06	Obj_BAI.1.2 追踪和报告变化状态	0.5	0.48	4.69			0.5	0.79	4.42
		Pro_DSS01	Obj_BAI.1.3 监督IT基础设施	0.5	0.66	4.54			0.125	0.67	4.08
Risk_BAI.2 IT 内部程序错误	0.86	Pro_BAI02	Obj_BAI.2.1 界定和维护业务功能和技术要求	1	0.82	4.00	系统于计划时的内部程序错误	APO	0	0.53	4.14
		Pro_BAI03	Obj_BAI.2.2 设计详细的解决方案元件	0.5	0.52	4.46			0.375	0.58	4.21
		Pro_MEA02	Obj_BAI.2.3 执行控制的自我评估	0	0.55	4.15			0	0.53	4.14
Risk_BAI.3 程序与控制	0.71	Pro_BAI06	Obj_BAI.3.1 追踪和报告变化状态	0.5	0.51	4.42	流程与控制制度建立上的问题		0.5	0.78	4.33
		Pro_DSS06	Obj_BAI.3.2 调整嵌入业务流程中的控制活动与企业目标	0.5	0.65	4.33			0.125	0.58	4.17
		Pro_MEA02	Obj_BAI.3.3 监督内部控制	0.5	0.67	4.42			0.5	0.67	4.42
Risk_BAI.4 程序错误	1.00	Pro_DSS02	Obj_BAI.4.1 验证批准,并满足服务请求	0.5	0.84	4.36					
Risk_BAI.5 作业系统的瑕疵		Pro_APO01	Obj_BAI.5.1 优化IT运作的位置	0	0.63	4.00			0.5	0.67	4.30

续表 3

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_BAI.5 作业系统的瑕疵	0.57	Pro_BAI09	Obj_BAI.5.2 管理关键资产	0.5	0.65	3.73	因作业系统的瑕疵而影响财务共享服务中心系统的运作		0	0.57	3.19
		Pro_DSS01	Obj_BAI.5.3 监督IT基础设施	0.5	0.50	3.64			0.375	0.63	3.80
Risk_BAI.6 信息系统或服务器的损坏	0.71	Pro_BAI09	Obj_BAI.6.1 确认和记录目前的资产	0.125	0.85	4.00	因信息系统或服务器的损坏而影响财务共享服务中心系统的运作		0.5	0.72	3.83
		Pro_BAI10	Obj_BAI.6.2 管理关键资产	0.625	0.95	4.00			0.125	0.58	4.17
		Pro_DSS04	Obj_BAI.6.3 建立和维护的结构资源和基准	0.125	0.58	3.83			0.625	0.79	3.92
			Obj_BAI.6.4 制定和实施业务持续性反应	0.25	0.74	4.00			0	0.60	4.00
Risk_BAI.7 意外的故障	0.71	Pro_APO01	Obj_BAI.7.1 优化IT运作的位置	0.125	0.67	4.08	因硬件或软件意外的故障而影响财务共享服务中心系统的运作		0	0.41	4.00
		Pro_BAI10	Obj_BAI.7.2 建立和维护的结构资源和基准	0.625	0.79	4.08			0.5	0.76	4.08
		Pro_DSS01	Obj_BAI.7.3 监督IT基础设施	0.5	0.72	4.17			0	0.58	4.00
Risk_BAI.8 大范围的组织变化	0.71	Pro_APO03	Obj_BAI.8.1 定义的参考框架	0.5	0.78	3.67	大范围的组织变化却未进行完善的变更管理作业		0.5	0.77	4.00
		Pro_BAI05	Obj_BAI.8.2 嵌入新方法	0.5	0.79	3.58			0.5	0.69	3.45
		Pro_MEA02	Obj_BAI.8.3 计划保证措施	0.5	0.90	3.50			0.5	0.69	3.45
Risk_BAI.9 缺乏版本更新的控制	0.71	Pro_BAI06	Obj_BAI.9.1 追踪和报告变化状态	0.125	0.58	4.17	因未有适当的IT人员而丧失版本更新的控制	APO	0.125	0.45	4.25
		Pro_BAI07	Obj_BAI.9.2 计划的业务流程，系统和数据转换	0	0.60	4.00			0.5	0.67	4.42
Risk_BAI.10 技术的误用	0.86	Pro_BAI04	Obj_BAI.10.1 评估目前的可用性、性能和容量，并建立一个基准	0	0.64	4.08					
Risk_BAI.11 流程再造的问题	0.71	Pro_BAI06	Obj_BAI.11.1 追踪和报告变化状态	0.25	0.90	3.92	因流程的再造而未进行变更管理		0.5	0.60	3.77
		Pro_BAI07	Obj_BAI.11.2 计划的业务流程、系统和数据转换	0.125	0.67	4.08			0	0.64	4.08
		Pro_DSS06	Obj_BAI.11.3 调整嵌入业务流程中的控制活动与企业目标	0.625	0.79	4.08			0.5	0.60	4.23

续表 3

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_BAI.12 缺少有效率的项目管理技术	0.86	Pro_BAI01	Obj_BAI.12.1 维护计划和项目管理的标准方法	0.5	0.65	4.38	因缺少有效率的项目管理技术而未达成变更管理	APO	0.5	0.63	4.31
Risk_BAI.13 流程再造的问题	1.00	Pro_APO06	Obj_BAI.13.1 创建和维护的预算	0.375	0.73	4.07					
		Pro_BAI09	Obj_BAI.13.2 管理关键资产	0.5	0.77	3.86					
Risk_BAI.14 现有系统准备变更的程度	1.00	Pro_BAI05	Obj_BAI.14.1 建立希望改变	0.875	0.83	3.93					
		Pro_BAI07	Obj_BAI.14.2 评估、优先考虑和批准变更请求	0.375	0.73	4.07					
		Pro_DSS04	Obj_BAI.14.3 进行恢复后检查	0.375	0.73	3.93					
Risk_BAI.15 缺乏信息基础建设	0.86	Pro_BAI01	Obj_BAI.15.1 识别和记录流动资产	0.5	0.87	3.62	缺乏信息基础建设，如防火墙、无线网络等		0.5	0.60	3.77
		Pro_BAI10	Obj_BAI.15.2 建立和维护的结构模型	0.5	0.78	3.46			0.5	0.78	3.46
Risk_BAI.16 无法支援资料整合的跨组织设计	1.00	Pro_APO03	Obj_BAI.16.1 定义架构的实施	0.375	0.86	3.86					
		Pro_APO04	Obj_BAI.16.2 建议一个有利于创新的环境	0.5	0.94	3.57					
		Pro_BAI05	Obj_BAI.16.3 启用操作和使用	0.375	0.58	3.79					
		Pro_BAI08	Obj_BAI.16.4 评估和删减信息	0	0.77	3.86					
Risk_BAI.17 缺乏资料库基础建设	0.86	Pro_APO03	Obj_BAI.17.1 提供企业基础架构服务	0	0.80	3.85	因缺乏资料库基础建设而影响财务共享服务中心系统运作		0.5	0.63	3.69
		Pro_BAI05	Obj_BAI.17.2 识别和记录资产						0.5	0.65	3.62
Risk_BAI.18 试图与旧系统结合	0.86	Pro_BAI09	Obj_BAI.18.1 保持的变化	0.5	0.80	4.15	与旧系统结合时未舍弃旧有系统而造成的问题		0	1.01	3.77
		Pro_BAI05	Obj_BAI.18.2 追踪和报告变化状态	0.5	0.52	4.46			0	1.07	3.85
		Pro_BAI07	Obj_BAI.18.3 计划的业务流程、系统和数据转换	0.5	0.66	4.46			0.5	0.65	4.38
		Pro_DSS01	Obj_BAI.18.4 执行操作的程序	0.5	0.60	4.23			0.5	0.60	4.23

表 4　　风险管理机制模型——DSS层面

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_DSS.1 存储媒介的处理	0.86	Pro_DSS05	Obj_DSS.1.1 管理IT资产的存取	0.5	0.85	4.31	存储媒介未做适当的管理而造成的问题		0.125	0.58	4.17
		Pro_DSS06	Obj_DSS.1.2 保护信息资产的安全	0.5	0.65	4.62			0.5	0.67	4.50
Risk_DSS.2 不受管束或未经授权的系统存储	0.86	Pro_DSS05	Obj_DSS.2.1 管理用户身份和逻辑存取	0.5	0.66	4.46	不受管束或未经授权的系统存取	APO	0.5	0.66	4.46
		Pro_DSS06	Obj_DSS.2.2 管理角色、职责，以及存取权限和级别的权限	0.5	0.65	4.38			0.5	0.52	4.46
Risk_DSS.3 缺乏交易轨迹	0.86	Pro_BAI07	Obj_DSS.3.1 计划的业务流程，系统和数据转换	0.5	0.86	4.08	缺乏经由计划与建立的交易轨迹	APO	0.5	0.48	4.31
		Pro_DSS04	Obj_DSS.3.2 定义业务持续性政策、目标与范围	1	0.95	3.92			0	0.55	4.15
		Pro_DSS06	Obj_DSS.3.3 确保信息事件和责任的可追溯性	0.5	0.66	4.54			0.5	0.66	4.54
		Pro_MEA01	Obj_DSS.3.4 建立一个监督方法	0.5	0.87	4.38			0.5	0.51	4.38
Risk_DSS.4 交易由电脑自动生成或执行	0.86	Pro_DSS01	Obj_DSS.4.1 管理设备	0	1.17	3.77	电脑自动产生交易，未经复核		1	0.86	3.92
		Pro_DSS06	Obj_DSS.4.2 确保信息事件和责任的可追溯性	0.5	0.80	4.15			0.5	0.75	4.31
		Pro_MEA02	Obj_DSS.4.3 执行控制的自我评估	0	0.76	4.08			0.5	0.73	4.23
Risk_DSS.5 人工控制依赖电脑控制	0.71	Pro_APO13	Obj_DSS.5.1 界定和管理信息安全风险处理计划	0.5	0.62	4.25	人工控制过度依赖电脑控制，存在发生舞弊的可能		0.5	0.67	4.36
		Pro_DSS01	Obj_DSS.5.2 监控IT基础设施	0.125	0.85	4.00			0.25	0.60	3.82
		Pro_DSS06	Obj_DSS.5.3 管理错误和异常	0.5	0.67	4.42			0.5	0.67	4.36
		Pro_MEA02	Obj_DSS.5.4 执行控制的自我评估	0.125	0.67	4.08			0	0.54	3.91
Risk_DSS.6 无法将使用者需求转换成技术需求或快速满足使用者需求	1.00	Pro_APO08	Obj_DSS.6.1 协调和沟通	0.5	0.76	4.43					
		Pro_BAI08	Obj_DSS.6.2 使用和分享知识	0.375	0.73	3.93					
Risk_DSS.7 不合逻辑的处理	0.86	Pro_APO02	Obj_DSS.7.1 定义战略性计划和路线图	0.5	0.76	4.08	不合逻辑的操作，导致错误发生		0	0.64	4.08
		Pro_BAI08	Obj_DSS.7.2 识别和分类信息来源	0	0.86	3.92			0.5	0.69	4.15
		Pro_DSS02	Obj_DSS.7.3 界定事件和服务请求分类方案	0.5	0.76	3.92			0.5	0.80	4.15

续表 4

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_DSS.8 资料转换	0.86	Pro_BAI06	Obj_DSS.8.1 跟踪和报告变更状态	0.5	0.76	3.92	资料转换时发生错误而影响系统		0.5	0.69	4.15
		Pro_DSS01	Obj_DSS.8.2 执行作业程序	0.5	0.77	4.38			0.5	0.80	4.15
Risk_DSS.9 没有办法快速回应	1.00	Pro_BAI03	Obj_DSS.9.1 涉及详细的解决方案	0	0.64	4.08					
		Pro_DSS02	Obj_DSS.9.2 验证批准,并满足服务请求	0.375	0.58	4.21					
		Pro_DSS03	Obj_DSS.9.3 确定和分类问题	0	0.55	4.00					

表 5　　风险管理机制模型——MEA 层面

风险因子	CVR	影响流程	控制措施	四分位差	标准差	均值	修正风险因子	重新分类	四分位差	标准差	均值
Risk_MEA.1 缺乏持续的沟通	1.00	Pro_APO10	Obj_MEA.1.1 管理供应商关系和合约	0.5	1.07	4.07					
		Pro_DSS06	Obj_MEA.1.2 调整嵌入业务流程中的控制活动与企业目标	0	0.53	4.14					
		Pro_MEA03	Obj_MEA.1.3 确定外部的遵从性要求	0.375	0.47	4.29					
Risk_MEA.2 缺乏外部顾问	0.86	Pro_APO02	Obj_MEA.2.1 了解企业发展方向	0	0.71	4.00	缺乏顾问,无法监督评估系统内控的适当性		0	0.55	4.15
		Pro_BAI01	Obj_MEA.2.2 管理利益相关者的参与	0	0.86	3.92			0.5	0.69	3.85
		Pro_MEA03	Obj_MEA.2.3 最佳外部要求的回应	0	0.64	4.08			0	0.82	4.00
Risk_MEA.3 难以衡量绩效与效益	0.86	Pro_MEA01	Obj_MEA.3.1 设置性能和一致性的目标	0.5	0.73	4.23	难以衡量财务共享服务中心的绩效,以确保程序执行		0.5	0.75	4.31
Risk_MEA.4 难以持续评估新的技术	1.00	Pro_MEA01	Obj_MEA.4.1 收集并处理性能数据和一致性目标数据	0.375	0.86	3.86					
		Pro_MEA03	Obj_MEA.4.2 确定外部的遵从性要求	0.5	0.71	3.71					
Risk_MEA.5 缺少高管层支持	1.00	Pro_MEA01	Obj_MEA.5.1 建立一个监督方法	0.5	0.77	4.14					
			Obj_MEA.5.2 分析和报告性能	0.5	0.63	4.36					
Risk_MEA.6 无法检验处理过程	1.00	Pro_BAI07	Obj_MEA.6.1 规划验收测试	0.5	0.77	4.14					
		Pro_MEA01	Obj_MEA.6.2 分析和报告性能	0.375	0.58	4.21					
		Pro_MEA03	Obj_MEA.6.3 外部合规性确认	0	0.62	3.93					

控制措施进行一致性检验，对于四分位差大于0.6或标准差大于1的控制措施按照专家意见进行了修正，处理后的结果如下：①Obj_APO.15.2修订为“需要基于企业文化建立一个有利于创新的环境”；②Obj_APO.19.1与Obj_APO.19.2两项控制措施修订为一项“规划时考虑资源的分配并定期识别和记录资产”；③Obj_APO.10.2修订为“从企业流程再造的角度了解企业未来的发展方向”；④Obj_BAI.18.1与Obj_BAI.18.2两项控制措施修订为一项“持续追踪新旧系统整合时变革的状态”。被删除的风险因子Risk_APO.3对应有4项控制措施，另有4项控制措施修正为两项，最终剩余130项控制措施。

修正后的财务共享服务中心风险管理机制模型满足效度与一致性要求。因此，本文通过两轮的德尔菲问卷，构建的基于COBIT 5的财务共享服务中心风险管理机制已得到专家的一致认同，涵盖IT管理领域的四个层面、52项风险因子、130项控制措施（详见表2~表5）。

五、风险管理机制的有效性验证

本文以某汽车制造公司作为研究对象，通过结构化访谈验证所构建的风险管理机制的有效性。首先了解案例公司实施财务共享服务中心的情况，以及在实施过程中所遇到的困难和挑战；然后分析案例公司试用所构建的财务共享服务中心风险管理机制；最后与案例公司相关人员进行沟通，评估风险管理机制在财务共享服务中心风险管理中的有效性、不足之处与需要加强的部分。

（一）案例公司简介

案例公司是国内一家大型汽车制造企业，下属控股子公司30余家，拥有员工54000余人。公司产品主要针对国内消费者，同时也积极拓展海外市场，海外销售已初见成效。公司的信息系统配置为SAP系统，包含三大模块：配销模块、制造模块及财务模块。配销模块包括库存管理、采购管理、订单出货管理等功能；制造模块包括产品结构管理、工单管理、物料需求规划、产能需求规划、生产规划以及成本管理等功能；财务模块包括总账、应收账款、应付账款、现金管理、固定资产等功能。

（二）结构化访谈实施情况

本文以结构化访谈的方式验证所构建的风险管理机制的有效性，访谈过程中用录音记录完整的访谈内容。访谈对象为公司的副总经理与IT管理部负责人，他们均为公司财务共享服务中心的项目组成

表6　　案例公司财务共享服务中心在IT管理领域各层面可能发生的风险

	访谈对象的观点	对应的风险
APO层面	在规划阶段风险发生的可能性是最大的，因为财务共享服务中心是全公司人员都在使用的系统，所以跨部门整合的难度是最高的	Risk_APO.5难以整合各个部门
	当初规划时只考虑了功能方面的问题，未考虑专利等无形资产，但是规划阶段不能只考虑功能方面的问题	Risk_APO.13未寻求咨询顾问进行适当的规划
	除了规划整合，高管层的需求也要考虑，若没有理清高管需求，后续维护就有可能会发生问题	Risk_APO.20人力资源政策未改变而导致人员任用错误
	财务共享服务中心系统的导入只有作业单位的关键人员才会参与，这位关键人员能不能代表单位需要予以考虑，这也可能成为风险的来源	Risk_APO.20人力资源政策未改变而导致人员任用错误
	在导入财务共享服务中心系统时，咨询的顾问若只具备软件知识而不具备公司行业背景知识，就有可能产生问题	Risk_APO.17系统供应商端口在系统的取得、开发和维护上的问题
	项目经理负责管理导入的所有事项	Risk_APO.4角色职权未适当分工，造成权力过度集中
	在财务共享服务中心系统导入和实施过程中，公司职员虽然受到相关教育培训，但在实际运行中，仍有可能存在一些未被界定的行为导致异常情况的发生，如产生异常的资料或造成资料错乱的风险	Risk_APO.7缺乏充分的训练计划
BAI层面	使用者与咨询顾问对财务共享服务中心系统的理解存在差异，系统导入期顾问团队和使用者沟通需求，上线初期使用者会认可顾问的意见，但随着系统的逐渐实施，使用者与顾问的理念可能会产生差异。该问题在财务共享服务中心导入开始时很难发现，只有在财务共享服务中心系统运行一段时间后才会发现	Risk_BAI.3流程与控制制度建立上的问题
MEA层面	在监督阶段，最大的风险在于界定相关监督标准，因为这些标准会随着公司的发展而变化	Risk_MEA.1缺乏持续的沟通

员或负责人。访谈后不足的资料，以电子邮件和电话的方式进一步补充，用文字整理出访谈记录。

案例公司将财务共享服务中心的运行分为导入与维护两个阶段。在导入阶段，采用单独项目实施的方式进行，项目主管明确项目的时间、成本、目标与范围；在维护阶段，公司进行正常维护，年底确定需要进行后续调整的部分。表6按照COBIT 5中IT管理领域的四个层面总结了案例公司可能发生的风险。

（三）应对财务共享服务中心风险的控制措施

案例公司应对财务共享服务中心风险的控制措施主要包括导入前的规范与导入后的管理，具体措施如表7所示。

表7　　案例公司应对风险的控制措施

导入前的规范	对应的风险
在导入阶段会有相关的规范和宣传，以防止在实际运作时发生风险	Risk_APO.7 缺乏充分的训练计划
根据过去的经验进行培训，开始导入时，制定操作手册，并对作业面的操作进行教育培训及严格的规范	Risk_APO.7 缺乏充分的训练计划
导入后的管理	**对应的风险**
实际运作时，一定会有异常情况发生，这些异常可能是在导入阶段没有被发现，而且大多是作业层面的问题，针对这些异常状况制定强制性的规范进行管理	Risk_BAI.3 流程与控制制度建立上的问题

案例公司在财务共享服务中心系统导入后，采用以下四个步骤进行风险管理：风险发现、比较、追踪和监管。首先，由财务共享服务中心项目小组提出财务共享服务中心面临的风险，并提出解决方案；其次，将财务共享服务中心小组提出的风险与风险项目表进行比较，将与风险项目表不对应的风险项目直接列入表内或修改原有风险项目表，扩大其涵盖范围；再次，由财务共享服务中心项目小组追踪识别出风险；最后，将风险管理结果与进度向管理层报告。风险管理结果通常包括移除非风险项目、改变风险管控模式以及增加新项目。

受访者针对财务共享服务中心的风险管理程序进行了补充说明：①导入前，会针对系统权限制定相关的风险管理计划；②导入后，会针对实际运作中发生的异常，执行改善程序；③年度总结中，会重新分析当前风险。

（四）财务共享服务中心风险管理机制有效性评估

访谈前请受访者审阅并使用所构建的基于COBIT 5的财务共享服务中心风险管理机制，根据执行结果评价其有效性。本文按照财务共享服务中心风险管理的四个步骤（风险识别、风险评估、风险应对、监督与修正）进行结构化访谈。

1. 风险识别。针对模型中列示的52项风险因子，请访谈人员识别这些风险在公司中是否曾经发生或可能发生。访谈结果显示，APO层面有23项风险因子可能发生，其中有16项（16/23≈70%）一定会发生；BAI层面有16项风险因子可能发生，其中有8项（50%）一定会发生；DSS层面有7项风险因子可能发生，其中有6项（86%）一定会发生；MEA层面有6项风险因子可能发生，其中有2项一定会发生（33%）。总之，受访者认为，在IT管理领域四个层面的52项风险因子中有32项（62%）一定会发生，说明本文构建的风险管理机制在风险识别阶段是有效的。

2. 风险评估。Hughes等[29]认为风险因子本身无法识别风险，需要通过风险评估才能找到重要的风险。因此，访谈中邀请受访者按照影响程度的高、中、低不同等级评估四个层面的风险因子。评估结果显示，APO层面有5项风险因子被评为影响程度高，BAI层面有2项风险因子被评为影响程度高，DSS层面有1项风险因子被评为影响程度高，MEA层面有1项风险因子被评为影响程度高。影响程度高的风险因子有9项，影响程度中等的风险因子有13项，影响程度低的风险因子有10项，可选择优先处理影响程度高的风险因子。

3. 风险应对。针对9项影响程度高的风险因子，列出受访者认为控制效果“好”和“中”的控制措施（如表8所示），这些措施便是公司在遇到影响程度高的风险因子时，可优先采取的应对措施。

在监督与修正方面，目前公司进行的财务共享服务中心的风险管理，分为导入前的规范和导入后针对异常情况的管理。受访者表示，本文所构建的风险管理机制的效用在于能清晰地评价风险因子的重要程度，明确列示出所对应的控制措施，使得财务共享服务中心导入时可以迅速评估风险、制订周详的风险应对计划。因此，对案例公司相关人员的访谈印证了所构建的财务共享服务中心风险管理机制的有效性。

六、结论

本文以COBIT 5为基础构建了一个便于企业识别、评估、应对与控制财务共享服务中心风险的风

表 8　影响程度高的风险因子与对应的控制措施

影响程度高的风险因子	控制效果“好”和“中”的控制措施
Risk_APO.13 未寻求咨询公司进行适当的计划	(Obj_APO.10.2)确实了解企业的发展方向
Risk_APO.15 管理层提出的可能影响系统运作的公司文化问题	(Obj_APO.15.1)定义一个可供参考的框架 (Obj_APO.15.2)基于企业文化建立一个有利于创新的环境
Risk_APO.5 难以整合各个部门	(Obj_APO.5.1)协调与沟通
Risk_APO.7 缺乏充分的训练计划	(Obj_APO.7.1)确定关键的IT人员 (Obj_APO.7.2)能组织和理解信息,将其转化为知识
Risk_APO.18 团队组成不稳定	(Obj_APO.18.1)界定组织架构的实施
Risk_BAI.3 流程与控制制度建立上的问题	(Obj_BAI.3.1)追踪和报告变化状态 (Obj_BAI.3.2)控制活动嵌入业务流程中以符合企业目标 (Obj_BAI.3.3)监督内部控制
Risk_BAI.6 因信息系统或服务器的损坏而影响财务共享服务中心系统的运作	(Obj_BAI.6.1)确认和记录资产 (Obj_BAI.6.2)管理与系统有关的关键性资产 (Obj_BAI.6.3)建立和维护一个配置资源的知识库和标准
Risk_DSS.7 不合逻辑的操作,导致错误发生	(Obj_DSS.7.1)提出战略性计划
Risk_MEA.1 缺乏持续的沟通	(Obj_MEA.1.2)控制活动嵌入业务流程中以符合企业目标 (Obj_MEA.1.3)确定遵循外部需求

险管理机制,并分析财务共享服务中心的风险因子的类型与特征,评估各项风险因子的影响,讨论可采取的方式和措施以应对风险。

本文由文献归纳总结财务共享服务中心风险因子,运用德尔菲专家问卷法进一步补充完善,并根据COBIT 5的规范提炼出相应的控制措施,最终提出涵盖IT管理4个层面的52项风险因子,以及应对这些风险因子的130项控制措施。本文还运用案例企业结构化访谈的方法验证了所提出的风险管理机制的有效性。

本文与现有研究的差异在于,基于信息技术控制目标(COBIT 5),结合财务共享服务中心风险管理的特点建立风险管理机制,方便企业快速识别风险,采取措施积极响应与改善缺陷,充分发挥其风险管理效果。随着技术的不断进步,本文所构建的风险管理机制无法涵盖所有未来可能发生的风险,这既是本文研究的局限也是未来研究的方向。

主要参考文献:

[1] Van Grembergen W., S. De Haes. Enterprise governance of information technology: Achieving strategic alignment and value[M]. New York: Springer,2009:1~20.

[2] Wilkin C. L., R. H. Chenhall. A review of IT governance: A taxonomy to inform accounting information systems[J]. Journal of Information Systems,2010(1):107~146.

[3] De Haes S., R. S. Debreceny. COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities[J]. Journal of Information Systems,2013(1):307~324.

[4] 林斌,曹健,舒伟. 信息技术内部控制研究——基于COBIT5的分析[J]. 江西财经大学学报,2016(1):36~44.

[5] Kerr D. S., Murthy U. S.. The importance of the COBIT framework IT processes for effective internal control over financial reporting in organizations: An international survey[J]. Information and Management,2013(50):590~597.

[6] 王会金. 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[J]. 审计研究与经济研究,2012(1):16~22.

[7] Aloini D.,R. Dulmin,V. Mininno. Risk assessment in projects[J]. Information Systems,2012(5):183~199.

[8] Morris J. J.. The impact of enterprise resource planning systems on the effectiveness of internal controls over financial reporting[J]. Journal of Information Systems,2011(1):129~157.

[9] Lin H., Cefaratti M., Linda L.. Enterprise risk management,COBIT,and ISO 27002:A conceptual analysis[J]. Internal Auditing,2012(2):3~12.

[10] Coe M. J.. Trust services:A better way to evaluate IT controls[J]. Journal of Accountancy, 2005(199):69~75.

[11] Reghavan K. R.. Internal control and operational risk: FDICIA, Sarbanes- Oxley and Basel II[J].

Bank Accounting and Finance,2006(19):3~9.
[12] Tuttle B.,S. D. Vandervelde. An empirical examination of COBIT as an internal control[J]. International Journal of Accounting Information Systems,2007(4):240~263.
[13] Kaarst-Brown M. L., S. Kelly. IT governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT Function?[A]. Hawaii: International Conference on System Sciences,2015.
[14] Bin-Abbas H., S. H. Bakry. Assessment of IT governance in organizations: A simple integrated approach[J]. Computers in Human Behavior,2014(32):261~267.
[15] Jan L., E. Iveroth. Creating a global network of shared service centers for accounting[J]. Journal of Accounting & Organizational Change, 2011(3): 278~305.
[16] Knol A. J., H. G. Sol. Sourcing with shared service centers: Challenges in the Dutch government[A]. Geneva: European Conference on Information Systems 2011 Proceedings,2011.
[17] Huang S. M., W. H. Hung, D. C. Yen, I. C. Chang, D. Jiang. Building the evaluation model of the IT general control for CPAs under enterprise risk management[J]. Decision Support Systems, 2011(50):692~701.
[18] Marijin J., A. Joha, J. V. Grinsven. Operational risk management as shared service center of excellence[M]. Fokker: Springer Fachmedien Wiesbaden,2013:363~378.
[19] Martin. W.. Critical success factors of shared service projects-results of an empirical study[J]. Advances in Management,2011(14):21~26.
[20] Owens. A.. Improving the performance of finance and accounting shared service centers[J]. Journal of Payments Strategy & Systems,2013(3): 250~261.
[21] Spears J. I., Barki H.. User participation in information system security risk management[J]. MIS Quarterly,2010(3):503~522.
[22] 何瑛,周访.我国企业集团实施财务共享服务的关键因素的实证研究[J].会计研究,2013(10): 59~66.
[23] 张瑞君,陈虎,张永冀.企业集团财务共享服务的流程再造关键因素研究——基于中兴通讯集团管理实践[J].会计研究,2010(7):57~64.
[24] 王光远,时现.全球信息系统审计指南[M].北京:中国时代经济出版社,2010:17~98.
[25] Linstone H. A., M. Turoff. The delphi method: Techniques and applications[M]. Massachusetts, M. A.: Addison-Wesley,1975:3~12.
[26] McKenna H. P.. The Delphi technique: A worthwhile approach for nursing?[J]. Journal of Advanced Nursing,1994(19):1221~1225.
[27] Lawshe C. H.. A quantitative approach to content validity[J]. Personnel Psychology, 1975(28):563~575.
[28] Holden M. C., J. F. Wedman. Future issues of computer-mediated communication: The results of a Delphi study[J]. Educational Technology Research and Development,1993(41):5~24.
[29] R. T. Hughes, Al-Shehab A. J., G.Winstanley. Using causal mapping methods to identify and analyses risk in information system projects as a post-evaluation process[A]. Amsterdam: European Conference on Information Technology Evaluation, 2004.
作者单位:河北大学管理学院,河北保定071002