国外SAP系统审计思路与经验启示

唐志豪(博士)　刘　瑾

(浙江财经大学信息学院　杭州　310018)

【摘要】本文从审计对象、目标、流程和内容四个维度归纳比较美国信息系统审计与控制协会与澳大利亚审计署的SAP系统审计经验,以此构建我国SAP系统审计框架,提出输入控制、处理控制、接口控制、访问控制、变更管理和职责分离审计是SAP审计的重点内容,最后通过实务案例表明该框架具有较好的合理性。

【关键词】SAP系统审计　国际经验　信息系统审计

SAP系统是利用现代信息技术,对企业人、财、物和信息资源进行统一集成管理的平台,通常包括销售和分销SD、物料管理MM、财务会计FI和人力资源HR等子系统。SAP系统的实施应用,在提高组织运营效率的同时,也带来内部控制重点的转移,并引发新的IT控制风险。相应的,SAP环境下的内部或独立审计的流程、内容和技术方法都会发生改变。对信息系统风险进行分析通常成为整个审计活动不可缺少的一部分,调阅SAP系统的业务流程设计文档、操作手册等文档,利用系统测试、计算机辅助审计技术等方法成为获取审计证据的常见形式。本文通过总结美国信息系统审计协会(ISACA)与澳大利亚审计署(ANAO)的国际经验,进而构建我国SAP系统审计框架,为相应实践提供可操作的参考。

一、国外SAP系统审计经验

(一)ISACA的SAP系统审计经验

ISACA是作为独立的外部审计组织,已开展多年的企业SAP系统审计业务。ISACA通过发布专门的SAP系统审计指南《Security, Audit and Control Features》来指导具体审计过程,以确定信息系统和相关资源是否受到充分保护、是否能保障数据和系统的完整性、是否能提供相关和可靠信息。

1. 审计流程。ISACA将审计流程分为事前检查阶段、初步审计阶段、详细审计阶段与报告阶段。事前检查阶段审计人员通过查阅系统开发与设计阶段的重要文档、观察数据库与应用程序服务器运行环境、评价备份与恢复计划有效性等措施了解企业。在初步审计阶段识别SAP系统的运行环境与关键控制。整个审计流程中最重要的阶段为详细审计阶段,根据组织的关键业务流程对具体系统应用控制进行实质性测试以判断相关业务的处理逻辑是否正确。在进行具体业务循环审查后通过分析控制成熟度,使利益相关者认识到组织现有控制水平与最佳实践的差别,体现内部控制的建立与优化。

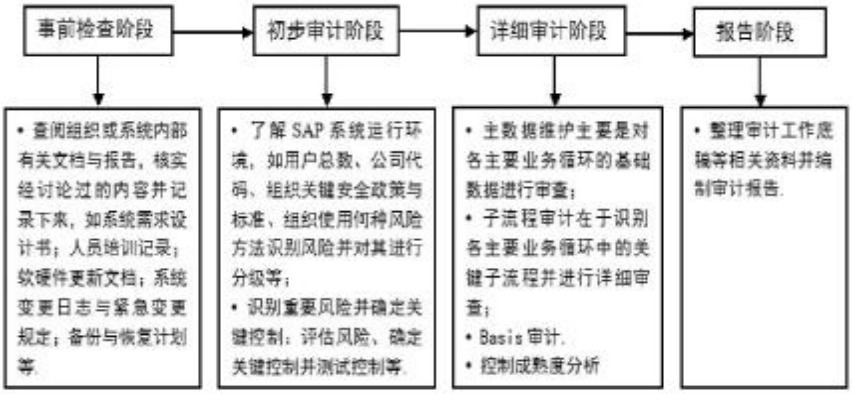


图1　ISACA审计流程图

2. 审计方法。SAP系统环境下仅依靠传统的审计方法如访谈法、观察法、文档查阅法来评估风险与控制显然是不充分的。随着系统内部信息资源量迅猛增加,获取审计证据的手段也面临革新。ISACA在实务中经常使用以下几种审计技术:

(1)数据挖掘技术。数据挖掘能够探测控制薄弱点并提供具体信息,从庞大的数据中发现有特殊意义的"知识",其最大的优点是能够及时取得充分可靠的审计证据,降低审计风险。数据挖掘工具种类繁多,从经济实惠的通用工具Microsoft Access、Excel到价格昂贵的专门工具如Audit Control Language(ACL)、Interactive Data Extraction and Analysis(IDEA),满足了不同审计需求。

(2)连续审计技术。连续审计技术借助于自动执行的程序实施数据抽取和分析,使审计人员在事件发生的同时掌握可靠的报告信息,通过对嵌入式审计模块和连续审计代理技术的运用能实现对数据的自动化截取与处理,有效保证审计信息的时效性。

(3)数据库活动监控技术。数据库活动监控技术(DAM)对后台数据库数据提供主动监控功能,避免问题数据的传输,并且能够及时通知事件相关用户。DAM节约了在数据服务器上的花费,加快了处理速度。

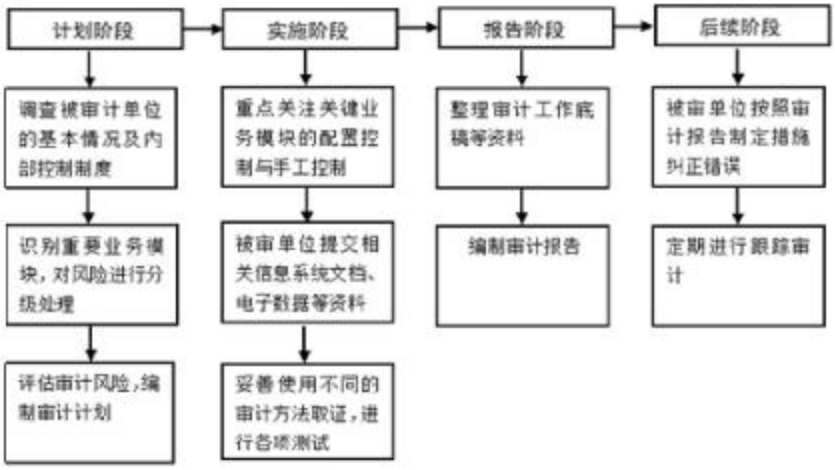


图 2 ANAO审计流程图

3. 审计内容。ISACA从组织控制环境、风险评估、控制活动、信息与沟通、监管的角度出发对企业收入循环、支出循环、Basis开展了一系列审计活动。

(1)收入循环。收入流程中主要评价主数据维护、销售订单处理、发票处理和现金收据处理等环节控制手段的强健性,其具体内容有:对主数据的变更操作是否合理、完整、准确;是否将主数据创建与变更的职责进行了分离。

(2)支出循环。支出循环中除了对主数据维护保持同样的谨慎态度外,还应在采购流程、支付流程上重点关注,如是否对输入、变更、取消、审核、支付供应商款项的职能进行职责分离;是否只对已接收货物或服务支付款项等。

(3)Basis。Basis是企业安全有效运行SAP系统的基础,包括系统应用程序安装、完善、运行、安全等内容。比如审查是否限制对Implementation Guide的访问、是否恰当设置系统参数以满足组织环境的要求。

(二)ANAO的SAP系统审计经验

与ISACA的独立审计不同,ANAO作为政府审计机关主要对政府部门开展SAP系统审计。澳大利亚各政府部门财政资金收入的80%与支出的70%都通过SAP系统运作,因此SAP系统的安全、可靠和有效运行对于政府部门的正常运转非常重要。为此,ANAO颁布了《Security and Control Update for SAP R/3》、《SAP ECC 6.0》等一系列指导手册,通过风险评级与流程控制保证了SAP数据流动过程的完整性、正确性与安全性。

1. 审计流程。ANAO的SAP系统审流程分为审计计划阶段、审计实施阶段、审计报告阶段和审计后续阶段。审计计划阶段初步了解被审计单位环境与内部控制制度,对关键模块的控制风险进行分级处理。审计实施阶段通过熟悉业务流程与系统文档,结合配置手段对系统数据执行各项实质性测试。在出具最终审计报告之后,定期进行跟踪审计保证对审计对象的适时评价、持续监督和及时反馈。

2. 审计方法。

(1)系统测试法。ANAO直接调用SAP系统的t-code代码查询获取数据,比如系统内部各类预定义的各种报表,通过对SAP系统产生报表的审阅,能够侦查系统异常情况或控制漏洞,便于发现违规行为。

(2)嵌入式审计模块法。AIS(Audit Information System)是嵌入在SAP系统中的审计模块,包括系统审计与业务审计两个子模块。系统审计模块主要用于管理活动与制度,为用户提供SAP安全控制报告与审计轨迹。业务审计模块便于审计人员编制资产负债表,并执行总账、应付账款和应收账款等关键账户的查询功能。

3. 审计内容。政府部门与企业所用SAP系统模块不尽相同,ANAO的SAP系统审计主要关注采购与应付账款、总账、人力资源管理等业务流程。

(1)采购与应付账款审计。采购流程包括采购申请、供应商选择、采购订单处理、货物收据、发票处理、支付处理等子流程,与应付账款管理密切相关。对该模块重点关注:建立订单是否有相关合同或协议做支撑、变更采购申请或采购订单细节是否服从适当审批程序等。

(2)人力资源管理审计。人力资源管理模块主要包括人事管理、工资计算等子流程,重点审查员工固定数据维护(Standing Data)、员工上岗与离岗记录、员工工时记录、薪金和福利计算、执行组织计划与人员招募等内容。比如是否采取控制手段保证员工主数据的完整性、员工离职后的信息是否仍处于激活状态等。

(3)总账审计。总账作为财务会计(FI)模块重要组成部分记录组织所有业务交易,与各类信息整合后最终生成资产负债表。审计人员对组织总账控制有如下关注:是否将总账维护与登账职责充分分离、是否对总账参数配置设置完整等。

(三)国际经验比较

通过对ISACA和ANAO有关SAP系统审计流程、内容与方法的总结,美澳在审计内容、控制手段、审计方法上有共通之处。在内容上,将ISACA的费用循环审计与ANAO采购及应付账款审计比较来看,费用支出交易大部分与采购订单有关,结合两者共性能概括采购及费用支出类交易的关键控制点,并用于实务操作。在具体控制手段上,两者都涉及变更管理、访问控制、职责分离、输入控制、处理控制、接口控制等,比如在输入控制中只有被授权的个人才能输入并审核准确的数据、在处理控制中合理限制对数据和信息的访问、在参数控制中保证设置变更的合理性。在审计方法上,除了采用传统方法,两者大多使用计算机辅助审计技术获取可靠证据。

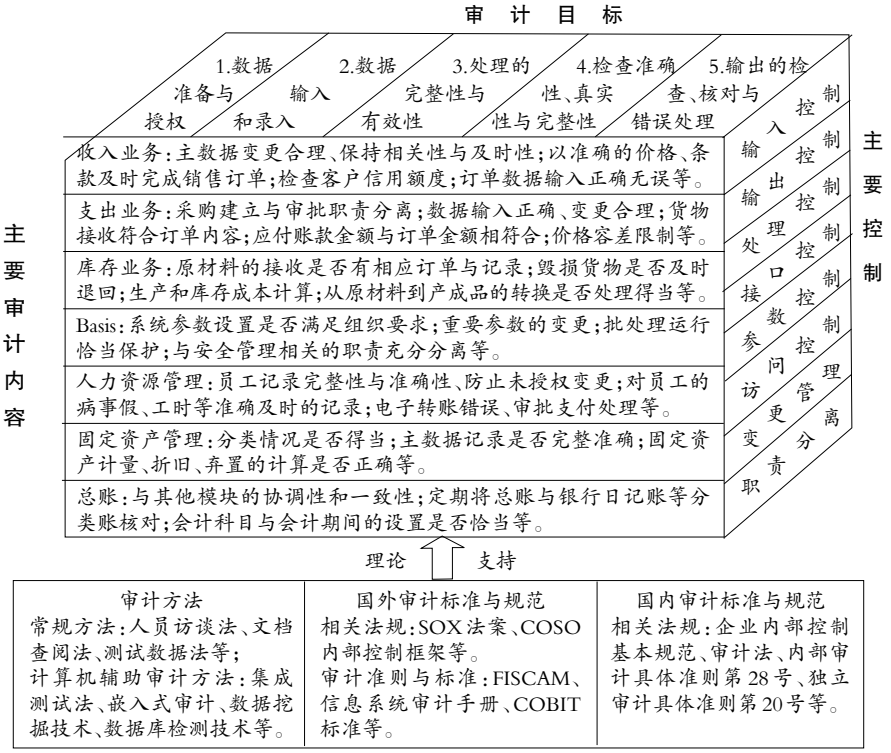
由于组织类型、规模、功能的差异,SAP系统的应用要求也有所不同。比如在审计内容上,因澳大利亚政府收入来源主要为国家拨款与项目基金,几乎不存在与销售货品相关的业务,据此ANAO弱化了与销售收入相关的审计活动,而ISACA将其视为关键环节。

表1　　ANAO与ISACA审计的比较

	ISACA	ANAO
审计对象	企业	政府机构
审计目标	避免由于信息泄露、资产损失、违法违规而带来的风险	提高对SAP系统安全与控制的风险意识
审计流程	事前检查—初步审计—详细审计—报告	计划—实施—报告—后续跟踪
审计内容及控制手段	支出循环与采购及应付账款	
	费用循环、收入循环、库存循环、Basis	人力资源管理、总账、固定资产管理
	输入控制、处理控制、接口控制、变更管理、职责分离、访问控制等	
审计方法	访谈法、文档查阅法、系统测试法、运用计算机辅助审计技术	

二、我国SAP审计框架体系构建

目前国内涉及信息系统应用控制层面的相关指导有国家审计署颁布的《信息系统审计指南——计算机审计实务公告第34号》、中国内部审计协会颁布的《中国内部审计具体准则第28号——信息系统审计》等,其应用要求分别属于强烈推荐遵循层次与非强制性层次,更高级别的强制性要求准则尚未发布,而在这些指南中,SAP系统审计相关内容还有极大的丰富与细化空间。在实务方面,我国众多大型企业如中石油、中石化、联想、海尔、国家电网等已经普遍使用SAP系统,为有效管理和使用SAP系统、更好实现经济监督职能,亟待一套相对完整并专门针对SAP系统的审计框架体系来指导实践活动。



SAP审计框架体系图

如上图所示,笔者尝试构建涵盖审计目标、审计内容、审计方法等在内的SAP系统环境下的审计框架体系并重点介绍主要控制手段。

1. 变更管理。变更活动主要有以下两种:一是对具体业务活动进行变更,如变更订单金额、数量、付款单位等信息,该类型变更会削弱交易过程的真实性和完整性,通过分析比较系统产生变更报告与已审批变更文档,可以有效避免此类现象发生;二是对系统配置进行变更,SAP系统提供了大量有效的系统配置(Configuration)功能,基于SAP系统设置可变更(Configurable settings)的特点,通过定期审核设置变更日志(Change Documents Log)并保证变更管理控制的充分执行,可以有效消除非法变更。

2. 访问控制。在SAP系统中,应在"最小授权原则"的基础上通过设置行为分配各种权限。物理访问是用来保护组织使其免受非授权访问的一种措施,要对计算机场所附近等所有可能出现物理访问风险的地方都建立有效的控制措施。

3. 职责分离。SAP系统环境下职责分离能够避免由于个人负责多个关键职位而产生不正当交易风险,是预

防欺诈及恶意行为的重要控制手段，如采购文件的创建与批准不能由同一人执行，以防止产生虚拟订单并被用户非法掩盖，影响采购流程的进行。在对职责分离控制进行分析时，注意不能只考虑某一模块内部的职责分离，而忽略了与其他相关模块的关联和系统外部的手工控制活动。

4. 接口控制。SAP系统内部模块数量较多，数据在模块与模块之间的传递与转换是系统整合的重点控制环节，有效的接口控制能够保证接口数据的完整性、安全性和准确性。如总账系统中，财务报表应付职工薪酬一栏中的数据来源于人力资源管理模块的工资单处理数据，应充分保证两模块数据间的协调一致性，并定期审查相关接口控制和SAP系统提供的对账报告。

5. 输入控制。数据一般通过键盘手工输入或系统导入等方式进入系统，输入错误的原因有人为失误或伪造数据、硬件机械故障、缺乏数据验证措施等，会导致应用程序系统产生非预期结果。在实务中可以审查以下内容：系统输入规则、数据采集标准等政策文件；数据输入校验机制是否有效、数据输入错误处理功能是否有效等。

6. 处理控制。对处理的控制应参照组织业务流程图以识别关键风险控制点，评估系统业务设计合理性与勾稽关系，分析系统运行逻辑，对错误处理机制进行评价。如采购订单建立是否经历了订单申请、订单审核过程；是否对订单进行功能性分级授权以限制订单变更操作等。

7. 参数控制。参数设置分为系统参数设置与业务参数设置。系统参数设置一般发生在系统初始化过程，如SAP系统中对用户角色类型、员工编号规则、销售订单字段等内容的设置；业务参数设置在系统运行过程中经常发生，如双重授权（Dual Authorisation）控制功能的开启。对参数的任何改变都会影响系统工作和内部控制的执行，因此所有参数变更操作将受到严格的审批与控制，应结合组织政策和业务流程审查参数设置情况以保证系统的正常运行。

三、实务案例

下面以某集团公司SAP系统审计实务为例，详细描述相关审计内容与流程。该公司以生产资料流通为主业，经营范围涉及国内外贸易、现代物流、流通加工等领域，自20世纪90年代起开始大规模进行信息化建设，现今已成功上线销售与分销（SD）、物料管理（MM）、财务会计（FI）、管理会计（CO）、财产管理（AM）、人事管理（HR）、项目管理（PS）等多个模块，这些模块建立在统一的数据平台之上，共包括约20 000张数据表，字段超过200万个，数据结构相当复杂。

根据被审计单位风险环境与SAP系统审计框架的审计目标，审计人员重点关注了系统的可靠性与安全性，警惕系统缺陷与漏洞，督促企业加强对信息系统的经营管理并提高系统运行的效率。对部分重点审计内容和具体过程描述如表2所示。

表2　　某公司SAP系统审计重点内容

审计内容	审计事项	审计实施程序
销售收款流程	信用管理岗位职责分离审计	查阅被审单位的业务流程设计文档与操作手册；使用t-code代码调用内部报告；访谈或现场观察等方式获取被审单位的职责分离控制状况
	销售最低限制价格审计	查看用户价格数据维护的权限与变更审计策略；查看容差设置情况
采购付款流程	业务岗位职责分离审计	查阅SAP系统采购付款流程设计文档；获得被审计单位的权限角色文档；获得系统账户的权限信息；根据关键职责分离控制要求，进一步分析权限测试结果中的账户与用户信息
	付款申请程序审计	查阅发票校验流程设计文档；在SAP系统测试机上执行发票预制程序
	发票冻结审核审计	查阅系统付款流程设计文档；在SAP系统测试机上修改某供应商的信用数据等
参数配置审计	系统参数变更审计	访谈参数维护的管理人员、查阅参数变更文档或调整日志
应用安全审计	访问权限审计	根据系统测试法查阅权限账号并查阅系统权限报告，访谈特权用户

1. 销售收款循环审计。审计小组通过查阅被审单位的业务流程设计文档与操作手册、使用t-code代码调用内部报告、访谈或现场观察等方式获取被审单位的职责分离控制状况，发现被审单位信用调查与合同审批权限由同一人掌握，削弱了销售过程的真实性。

2. 采购付款循环审计。审计小组通过查阅被审计单位SAP系统的付款流程设计文档、在SAP系统测试机上修改某供应商的信用数据并运行付款申请功能模块，发现该功能模块不能调用供应商信用数据，后续的付款审批和付款执行都不由供应商信用数据控制。结果表明付款申请功能模块设计与开发存在错误。

3. 参数配置审计。审计小组通过访谈参数维护的管理人员、查阅参数变更文档或调整日志，核查异常情况。结果表明该公司对员工工资等个别参数的调整在数据库上直接操作，且不记录操作轨迹，不利于数据安全。

4. 安全审计。审计人员检查了有权限访问“用户维护”的用户、有权限维护关键或自定义表格的用户及超级用户SAP*功能是否失效，据此判断系统是否运行安全。

【注】本文由中国博士后科学基金（基金号：2012M520321）资助。

主要参考文献

1. 唐志豪，吴叶葵.RTP环境下采购付款业务流程控制的审计.财会月刊，2012；12

2. 宋贻生，徐琼芳.提升信息化环境下大型项目的审计能力.审计月刊，2014；1