

联合国儿童基金会信息系统审计的实施与特点

李庭燎¹, 王洁²

(1. 南京审计学院 信息科学学院, 江苏 南京 211815; 2. 审计署济南特派员办事处, 山东 济南 250011)

[摘要] 信息系统审计是控制组织中信息系统风险、保证组织业务正常运行、实现业务目标和提高组织竞争力的重要途径。联合国儿童基金会的信息系统审计, 调查总结了当前联合国儿童基金会信息系统的现状及实施信息系统审计的过程、内容和技术方法, 体现了境外信息系统审计重视程序规范、重视绩效和审计沟通的特点。

[关键词] 信息系统; 信息系统审计; 联合国儿童基金会; 管理审计; 计算机审计

[中图分类号] F239.65 **[文献标识码]** A **[文章编号]** 1672-8750(2012)01-0058-05

信息系统审计是控制组织中信息系统风险、保证组织业务正常运行、实现业务目标和提高组织竞争力的重要途径, 目前针对国外组织的信息系统开展的审计工作还不多见。联合国儿童基金会的信息系统审计实施的过程、内容和技术方法, 体现了境外信息系统审计重视程序规范、绩效和审计沟通的特点。作为儿童基金会信息系统审计领域的主要人员, 笔者意图通过对儿童基金会信息系统的具体情况、审计内容、审计方法、审计过程和特点的述评, 为我国开展信息系统审计在流程、内容与方法上提供借鉴。

一、联合国儿童基金会信息系统现状

(一) 联合国儿童基金会的基本情况

联合国儿童基金会(以下简称儿基会)成立于1946年, 1953年成为联合国系统的常设机构, 是联合国大会的下属机构, 主要职责是对发展中国家的母亲和儿童进行长期的人道主义和发展援助, 其具体工作涉及191个国家的项目和活动^[1]。儿基会的组织结构分为纽约总部、七个地区总部以及众多国家办公室三个层次, 此外还设立了36个国家委员会。

儿基会开展的项目主要围绕四个领域展开: (1) 儿童生存、增长和发展情况; (2) 优质教育和两性平等; (3) 艾滋病病毒、艾滋病防治; (4) 保护儿童权益^[2]。其业务涉及对一百多个国家办事处的日常运营管理和项目的支持。

(二) 联合国儿童基金会信息系统的现状

儿基会总部的日常业务管理主要通过遍布全球的信息系统来实现, 组织的业务对信息系统的依赖性非常强, 每一项具体业务的开展, 包括财务管理、人力资源管理和后勤采购管理, 都需要信息系统支持。信息系统在提供对业务支持的同时, 也存在巨大的潜在风险。儿基会总部的IT部门是保障组织业务运行的关键核心部门, 主要负责儿基会的IT整体架构的设计、管理以及内部多种信息系统的日常运

[收稿日期] 2011-07-15

[基金项目] 国家自然科学基金(70971067); 江苏省高校自然科学重大基础研究项目(08KJA520001); 江苏省高校优势学科“审计科学与技术”子项目(YSXKKT09); 南京审计学院校级课题(NSK2007/C14)

[作者简介] 李庭燎(1978—), 男, 河南平顶山人, 南京审计学院信息科学学院讲师, 东南大学经济管理学院博士生, 注册信息系统审计师, 主要研究方向为信息系统审计; 王洁(1976—), 男, 山东济南人, 审计署济南特派员办事处计算机审计处审计师, 主要研究方向为计算机辅助审计。

营维护。IT 部门主要有八个职能领域,涉及各个国家办事处的 ProMS 运行管理、业务系统整合、财务和人力资源管理、系统运营管理、技术架构、Internet 服务、全球通讯以及信息安全等具体职能^[3]。

1. 总部的主要信息系统

儿基会纽约总部有两个办公地址,分别位于联合国总部附近的两栋不同的建筑,通过光纤相联。每栋办公楼内有局域网和 DMZ 区,对服务器和开发区还设置了特定 VLAN。

儿基会的广域网包括三部分:通过 EMC 公司提供的基于卫星传递的 VSAT(Very Small Aperture Terminal)网络,通过 SITA 公司提供的 MPLS(Multi-Protocol Label Switching)网络,以及由当地 ISP(Internet Service Providers)提供的 IPSec VPN(Internet Protocol Security Virtual Private Networks)网络。

儿基会纽约总部使用的业务系统是基于客户需求定制的 SAP。1997 年儿基会通过竞标开发了自己的 ERP SAP 系统,自 1999 年开始投入使用,初期系统功能支持会计、预算、采购、仓库、贺卡销售等业务,在纽约总部、哥本哈根和日内瓦总部使用。2002 年 SAP-FLS(SAP-Financial and Logistics System)版本升级为 V4.5,新增了部分功能;2005 年又增加了 SAP 中的人力资源和工资模块。目前使用的版本是 SAP-FLS 6.0。

SAP-FLS 基于 Client-Server 结构,目前在纽约、哥本哈根、日内瓦、布鲁塞尔和区域办事处使用,实现数据及时通讯,具备总账管理、应收账款、应付账款、资金管理、成本控制、项目管理、差旅和后勤管理等功能。SAP-FLS 在 SAP R/3(Systems, Applications and Products)商业数据处理财务软件基础上开发而成,通过该软件可以实现业务处理过程的自动化,减少数据重复输入,并自动生成报告。

由于儿基会的国际雇员和总部工作人员的工资数据由联合国通过 IMIS 系统进行处理,因此在 SAP-FLS 中有一个特殊的接口可导入这些人员的工资数据。2005 年 11 月,儿基会在 SAP 中增加了工资模块,对捐献的资料管理和监控使用 Access 数据库。

2. 各个国家办事处使用的信息系统

除了总部之外,各个国家办事处使用的 ProMS(Programme Manager System,项目管理系统)是儿基会自行开发的、所有国家办事处统一使用的应用系统。ProMS v1.0 自 1998 年开始使用,目前使用的是 ProMS v8.51 版本,面向 165 个国家、220 个地方的约 4300 个用户。

ProMS 包括项目计划、项目管理、资金的分配和管理、采购管理、财务管理、人力资源管理、工资管理、出差管理、捐赠者报告管理等功能,是国家项目实施的主要日常管理工具。

每个国家办事处的远程数据库都是全球统一数据库的一部分,国家办事处数据的任何变更都会传送到总部的中心数据库,这样从纽约总部的数据库亦可访问国家办事处的数据。纽约或哥本哈根总部的数据(如采购分类、人员表、开支等)也可发送给各国家办事处。每个国家办事处都有 2—3 台服务器,其中一台专用于 ProMS。区域办公室因具有数据备份等功能,有十几台服务器。每年,儿基会都会考虑对国家办事处和总部的现有系统进行提升和完善,集成新的功能以适应新的业务需求。

按照儿基会的规划,2012 年,所有的国家办事处和区域办公室都将全面过渡到 SAP ECC6.0 系统的统一平台上,目前蓝图和设计阶段已经完成,正处于新版本系统的全面测试阶段。

二、联合国儿童基金会信息系统审计的实施过程

(一) 信息系统审计的内容

信息系统控制与审计协会认为,信息系统审计是获取并评价证据从而判断所评价的计算机系统是否能够保证资产安全、数据完整、实现组织目标并能够有效利用组织资源的过程^[4]。具体审计工作的开展,还需要根据情况对信息系统运行的效率、效果、可用性、可靠性、机密性、完整性、合规性等内容进行评价^[5]。这些内容通常可以归纳为三个层面:组织层面的 IT 治理问题,IT 支持层面的服务交付和服务支持,以及具体业务流程层面的应用控制^[3]。在具体的审计过程中,它需要对信息系统

设计、开发、实施、运营维护及绩效全过程进行分析,最终目标是对信息系统的合规性、安全可靠、功能有效性和资源利用绩效等方面做出评价。

(二) 儿基会信息系统审计的定位

对儿基会的审计工作包括采购、预算、项目管理、人力资源、差旅管理、财务控制、现金援助、信息系统、资产管理等十余个具体领域。通过调查我们了解到,信息系统对儿基会的日常业务开展起着关键的支持作用,信息技术部除了负责管理信息系统的运营和维护,还需要帮助其他业务部门解决在使用信息系统开展业务工作过程中遇到的各种问题。

儿基会信息技术部门每年的预算非常庞大,其中不仅涉及软件、硬件的购买和维护,还涉及服务管理、知识管理等内容。2008 年全年 IT 部门的预算高达 1200 万美元,其中软硬件的采购和维护约 200 万美元,更多费用是用于知识管理系统的建设以及功能模块的开发。

基于这种情况,审计人员对儿童基金会的信息系统审计不仅仅要关注开发的系统和软件本身,而且也需要关注信息系统对业务的影响,特别是要结合其他领域的问题分析信息系统是否真正满足对业务的控制要求,以及 IT 战略是否符合儿童基金会业务战略的 IT 治理问题。因此,对儿基会的信息系统审计,既是独立的审计领域,同时也为其他领域的业务审计提供支持和服务。

(三) 儿基会信息系统审计总体目标

在具体审计项目中,通过问卷调查,审计人员了解到儿童基金会的 IT 部门主要职责有三个方面:一是通过将 IT 与业务流程融合,帮助儿童基金会实现战略目标;二是通过提供完整、先进、高效和安全的系统解决方案,满足组织内部和外部伙伴的业务需求;三是确保提供的信息系统服务质量符合组织的要求。

根据前期调查的结果,审计人员结合该领域的主要业务特点和相关风险,确定了针对儿基会总部信息系统审计的总体目标,包括以下五个方面的内容:一是 IT 治理,主要评价组织 IT 战略与业务战略的关系,IT 战略、政策的制定是否规范、全面以及执行是否到位;二是资产保护,主要评价 IT 相关资产是否得到有效保护,数据中心物理和逻辑访问控制是否适当;三是系统安全,主要评价关键信息系统是否存在安全风险和薄弱环节;四是服务管理,主要评价 IT 部门的服务管理流程、措施和控制活动的有效性以及潜在风险;五是应用控制,主要评价关键业务流程中的授权和审批以及数据处理环节是否存在风险。

(四) 采用的技术和方法

在审计实施过程中,审计人员主要采用的审计方法和技术包括问卷调查、访谈、检查文档、实地观察、抽样和数据测试等。

1. 问卷调查法:通过发放调查问卷,获取有关系统资料,评价信息系统基本情况和管理制度的制定情况,确定需要评价的关键领域的风险和控制措施。

2. 访谈法:通过与相关部门的业务人员和管理人员面谈,评价 IT 政策和程序的制定和执行情况。

3. 检查文档法:通过检查文档和记录,评价 IT 相关政策的完备性、合理性、有效性及具体执行情况。

4. 实地观察法:通过查看物理环境和实际工作场所,评价数据中心等场所的运营管理情况。

5. 抽样分析:通过对系统中数据进行抽样检查和分析,判断有关业务的实际执行情况。

6. 测试法:通过数据测试,检查输入控制、处理控制和输出控制的情况。

(五) 审计事项的确立

审计人员根据问卷调查的结果,经过风险分析,在一般控制和应用控制方面确定了需要关注的五类风险点,涵盖 IT 治理、系统生命周期、资产安全、信息安全、业务流程控制等方面,具体内容见表 1。

表 1 主要审计事项

审计事项类别	审计事项子类	审计事项名称
一般控制审计	IT 治理	IT 战略和政策审计
	信息系统生命周期管理和控制	系统开发控制审计
	信息资产安全	物理环境控制
	信息安全管理 and 控制	逻辑访问控制审计
应用控制审计	业务流程控制	交易数据输入控制审计 数据处理逻辑审计

(六) 审计发现的主要问题

针对审计目标,我们从总体上得出五点结论:(1)IT 部门组织结构设置合理,IT 相关政策完备,更新及时,具有有效的控制环境;(2)数据中心的物理和逻辑控制符合业务要求,相关的 IT 资产采购管理规范,并有完善的审批制度;(3)IT 部门具有独立的系统开发、测试、运行环境;(4)IT 部门制定了针对变更管理的完整有效的授权和审批程序;(5)信息安全和运营维护有专门的部门负责,管理规范。

对儿基会的信息系统审计,审计人员也发现了其中存在的一些问题和风险,主要体现在系统开发控制、逻辑访问控制审计和应用控制方面。

系统开发控制方面,儿基会正在开发新的基于 SAP 的 One ERP 系统,用于整合总部与各地办事处的业务应用。该系统是核心的业务系统,为满足国际公共部门会计准则要求而设计建设,按计划将于 2012 年初正式运行。通过访谈调查,结合对计划进度安排分析,与实际执行情况进行对比,审计人员发现系统开发在工作进度安排上存在一定的问题和潜在风险,有部分开发项目未及时完成。

逻辑访问控制审计方面,儿基会制定了专门的信息安全管理指南,要求超过一年未登录使用系统的用户账号及时关闭。审计实施过程中,通过访谈和对处理流程的调查,审计人员初步判断信息系统账号管理存在风险。经过测试验证,审计人员发现确实有部分用户账号自创建后从未启用,且多个账号已超过一年未经登录使用,应予关闭而没有关闭。出现这种情况的主要原因是 SAP 系统的账号管理和人事部门人员信息更新之间存在脱节,导致系统存在被非授权人员登陆的风险。

另外,在应用控制方面,捐赠报告的数据输入和捐赠资金的数据处理上存在着数据输入控制不严格、数据处理控制错误等问题。

三、联合国儿童基金会信息系统审计的特点

比较儿基会信息系统审计的实施和我国国内审计的现状,我们发现儿基会信息系统审计具有三个主要特点。

(一) 以绩效为导向的管理审计,关注绩效

联合国在绩效管理方面制订了基准框架。联合国审计项目不仅在预算执行和财务收支审计方面突出了绩效审计的概念,在信息系统审计方面,也突出体现了这一点。IT 项目的进展直接影响到业务运行的成本和效率,因此对于 IT 项目管理的影响,审计人员要进行深入分析和评价。而且由于系统中的账号使用都需要许可证,多余不用的账号,既有安全的隐患,也会造成成本的增加,这也意味着预算编制可能存在潜在风险。绩效问题是目前国内审计的热点问题,把信息系统审计与绩效审计相结合,研究信息系统绩效的评价指标体系,将会是信息系统审计关注的重要内容。

(二) 与管理当局交流,重视沟通,关注审计效果

审计发现和落实是审计成果最直接、最具体的体现,它同时也体现审计的价值。联合国审计项目在整个审计过程中,通过与被审计单位在审计准备阶段的沟通,提前让管理层了解审计目标、审计范围、实施进度安排、所需提供资料等信息,最大程度地争取管理层的理解和配合;在现场实施过

程中,对于每一个审计发现,都积极运用有效的沟通与协调技巧,确保取得对方的理解和支持,促进整改落实,保证了审计质量,也达到了通过审计工作帮助被审计方改进的目的。

(三) 选择合适标准,注重程序的规范,体现质量管理

联合国审计的全过程都贯彻和体现了质量管理,制定了质量控制规范并严格对照执行,对每个具体事项都要求遵循“审计质量控制检查表”,体现了事前、事中和事后的全过程连续监督和控制。控制规范既是项目负责人进行自评自查的标准,也是联合国审计委员会对审计项目质量进行事后监督的重要依据。目前国内在信息系统审计领域还没有权威公认的指南和标准^[6],联合国儿童基金会审计中采用的国际公认的《信息系统相关技术控制目标》作为审计标准,也可作为国内开展相关审计工作的参考。

虽然信息系统审计目前是相对独立的审计领域,但实际上每个具体的审计领域几乎都离不开信息系统的评价和应用。儿童基金会的信息系统已经融入每一个具体的业务领域,无论是为了提高效率,还是为了识别新的风险,对具体业务领域的审计都要求对信息系统有充分的认识 and 了解。对儿童基金会开展信息系统审计是对审计人员的一次挑战,也是将信息系统审计理论应用于实践的有益尝试。在审计过程中发现的风险和积累的经验,对于国内的信息系统审计工作,具有一定的参考价值和启发意义。

参考文献:

- [1] 联合国儿童基金会. 关于联合国儿童基金会[EB/OL]. (2007-01-12) [2011-03-06]. http://www.unicef.org/chinese/about/who/index_history.html.
- [2] 李越冬. 议联合国儿童基金会国家办公室审计[J]. 审计与理财, 2009(6):58.
- [3] 李庭燎, 辛风. 联合国儿童基金会信息系统审计及其启示[J]. 中国内部审计, 2010(8):27-29.
- [4] 陈婉玲, 杨文杰. ISACA 信息系统审计准则及其启示[J]. 审计研究, 2006(S1):108-112.
- [5] 张文秀, 齐兴利, 黄溶冰. 基于 COBIT 的信息系统审计框架研究[J]. 南京审计学院学报, 2010(4):29-34.
- [6] 陈婉玲, 袁若宾. COBIT 及其在信息系统控制与审计中的应用[J]. 审计研究, 2006(S1):93-96.

[责任编辑:黄 燕]

The Implementation and Characteristics of Information System Audit in UNICEF

LI Ting-liao, WANG Jie

Abstract: Information systems audit is the important way to control IS risk, ensure the operation of the business, achieve business goals and enhance organizational competitiveness. The IS audit for foreign organizations is still blank at present. UNICEF information system audit summarized the current status of UNICEF's information system, introduced the contents, objectives and methods of the implementation process, and reflected the features of IS audit that concern procedural norms, performance and communication.

Key Words: information system; information system audit; UNICEF; management audit; IT audit