信息系统专业审计研究与实践

穆勇[1]，赵莹[1]，张燕生[2]，支俊辉[2]
（1. 北京市信息资源管理中心，北京 100101；
2. 航天世纪咨询有限公司，北京 100048）

摘　要　针对已建成或正在运行的大量信息系统中存在的系统与实际业务流程不匹配、数据不规范、信息共享难及系统与技术文档“两层皮”等方面的问题，首次引入了“信息系统专业审计”的概念，界定了其内涵和外延，创新性地提出了一套信息系统专业审计的定位、目标、对象、内容、依据、工具、方法、组织、策略、流程、成果及作用的体系框架，并对某市政府部门 28 个信息系统进行了专业审计，取得了良好效果。

关键词　信息系统专业审计，研究，实践

中图分类号　F239.1

1　引言

经过多年的信息化建设，我国政府部门和企业建成了大量的信息系统，在企业管理和公众服务等方面发挥了重要作用，但由于这些系统大都是在不同时期由不同厂商建设、运维的，加之多年来不断升级改造，普遍存在着系统与技术文档“两层皮”、系统与实际业务流程不匹配、功能与接口错综复杂难以把控、数据标准化程度差、信息共享难、业务系统和数据安全隐患高等问题。对此，如果任其发展，将会给后续系统的运维管理、升级改造和互联互通带来困难，但又不能一关了之。

为了解决上述问题，急需创新信息系统审计理论和方法，能够快速有效地找出系统问题，发现“僵尸”系统，整治系统乱象，助力系统整合，确保信息资产保值增值。

2　国内外 IT 审计理论研究与实践现状

2.1　国外 IT 审计研究与实践现状

IT 审计（也称为“信息系统审计”）出自 20 世纪 60 年代 IBM 出版的 *Audit encounters Electronic Data Processing*[1]，70 年代中后期到 80 年代初，由于计算机在发达国家的初步普及，利用计算机犯罪和计算机系统失效的事件频频出现，IT 审计日益得到社会重视，美国、日本先后成立了 IT 审计方面的协会组织，从事 IT 审计规则的制定和实施指导。90 年代是 IT 审计的普及期[2]，互联网的普及为计算机犯罪提供了温床，此外，日益严重的软件项目失败问题引发了是否要对信息系统的投资和开发进行审计的深思，IT 审计得到了前所未有的重视。1994 年，EDP（Electronic Data Processing，电子数据处理）审计师协会正式更名为信息系统审计与控制协会（Information Systems Audit and Control Association，ISACA），它是国际上唯一的 IT 审计专业组织，通过制定和颁布信息系统审计标准、指南和程序来规范 IT 审计师的工作[3]。

通信作者：赵莹，女，工程师，北京市信息资源管理中心项目主管。E-mail：zhaoy@bjeit.gov.cn。

目前，业内对于 IT 审计还没有一个统一的定义。国际 IT 审计领域的权威专家 Ron Weber[4] 将其定义为“收集并评价证据，以判断一个计算机系统（信息系统）是否有效做到保护资产、维护数据完整、完成组织目标，同时最经济地使用资源”。1996 年日本通产省情报处理开发协会信息系统审计委员会将其定义为“为了信息系统的安全、可靠和有效，由独立于审计对象的信息系统审计师，以第三方的客观立场对以计算机为核心的信息系统进行综合的检查与评价，向信息系统审计对象的最高领导层提出问题与建议的一连串的活动”。

随着信息技术在社会经济中的广泛运用，IT 审计的目标从对数据处理系统的正确性和可靠性进行审查发展到对整个信息系统的效率、可靠性、有效性和安全性的审查；审计的方法从手工审计发展到手工审计与计算机辅助审计工具和技术相结合；开展审计的人员从注册会计师发展到专门的 IT 审计师；指导 IT 审计的组织从传统的审计机关和组织发展成为专业的 IT 审计组织；IT 审计的内容、依据、准则等也随着信息技术和信息系统的发展而不断发展和完善[5]。

2.2 我国 IT 审计研究与实践现状

从 20 世纪 80 年代起，国内专家学者就开始尝试将国外的 IT 审计理论引入我国[6]。例如，关于 IT 审计的定义，潘晓江[7]提出“IT 审计是现代审计的有机组成部分，主要任务是检查会计信息系统数据的可靠性，检查资产保护的状况，数据处理工作的成效以及对系统内的人、财、物等各种资源的利用率”。唐清亮[8]提出“IT 审计的基本任务是通过计算机系统的检查、测试和评价，提供确切可靠的审计证据，以确定企业的经济活动是否符合党和国家的法律、法规，是否执行了党和国家的方针政策，企业的财务收支活动是否符合财经制度和纪律，是否存在违法乱纪活动，以及确定企业经济效益的高低”。这些理论虽然已经进行了一定程度的本土化改造，但在发展过程中证明，起源于国外的理论和方法与我国实际情况存在较多不适应，无法很好地指导我国信息系统审计实践[9, 10]。为了进一步规范信息系统审计行为，中国内部审计协会[11]于 2008 年发布了《内部审计具体准则第 28 号——信息系统审计》，但由于这些准则过于笼统，缺乏实施细则，难以真正指导审计实践[12]。

由于缺乏理论指导，目前国内的信息系统审计应用实践还很局限，主要是针对信息安全审计[13]和信息化项目审计[14]（偏重于财务收支审计）两方面，分别由安全测评部门和财务审计部门组织实施，而针对信息系统的技术文档、业务流程、数据规则、功能接口等方面的专业审计工作还基本处于空白[15]。同时，由于信息系统审计专业性较强，传统的审计手段、审计工具、审计人员难以满足信息系统审计的要求。

2017 年 5 月，国务院办公厅印发的《政务信息系统整合共享实施方案》（国办发〔2017〕39 号）明确提出“探索政务信息系统审计的方式方法”，“加快消除‘僵尸’信息系统”。在上述背景下，本文针对我国政务信息系统共享整合的特点和需求，对 IT 审计部分内容进行了裁剪，对重点内容进行了补充扩展，创新性地提出了与我国信息化发展相适应的信息系统审计的理论体系框架，有别于传统的 IT 审计，称为“信息系统专业审计”（information system professional auditing，ISPA）。

3 信息系统专业审计体系框架和主要内容

信息系统专业审计是一个系统工程，涉及众多复杂问题，需要建立一个完整的体系框架（图 1），该体系框架包括系统分类与系统数据采集、实施审计与查找问题、提出建议与系统整改方案、实施策略与保障机制、专业人员和专用工具等五大方面。本文重点针对信息系统专业审计的定义、定位、目标、对象、内容、依据、工具、方法、组织、策略、流程、成果及作用等方面进行阐述。

图 1 信息系统专业审计体系框架

3.1 信息系统专业审计的定义与定位

信息系统专业审计是指对已建并投入运行的信息系统技术文档、业务流程、数据、功能、接口、运维等按照国家和国际的相关标准规范进行合规性和一致性审计，补充完善相关技术文档，理清与修正系统业务流程、数据关系以及数据操作规则、交换规则和展示规则，并对系统的整体运行情况和效益给出审计意见和专业建议，审计报告将作为相关系统整合、数据迁移、共享交换、安全运行和运维管理等工作的重要依据。

“信息系统专业审计”是在国外 IT 审计理论基础上结合我国信息化发展的实际需求形成的本土化概念。与传统的 IT 审计相比，信息系统专业审计最大的不同点在于：传统的 IT 审计的目标是“发现问题，给出建议”，而对于信息系统专业审计，仅仅发现并指出信息系统存在的管理上和技术上存在的问题是不够的，还要针对发现的问题，由专业人员采用一套信息系统专业审计的方法和专用工具来帮助解决好这些问题，从而“根治”系统病灶，更好地保护已建信息资产。

3.2 审计目标、对象和内容

信息系统专业审计的目标体现在如下几个方面：一是发现技术文档存在的内容不完整、功能不一致、数据不正确等问题，并有针对性地补充完善相关技术文档；二是理清并修正现有系统开发与运行中的业务流程、系统功能、接口、数据关系和操作规则、交换规则、展示规则等方面的问题；三是对系统的运维效率、效能和效果进行审计；四是对系统整体运行情况和绩效给出审计意见和建

议，专业审计报告将作为相关系统整合、数据迁移、共享交换、安全运行和运维管理等工作的重要依据。

信息系统专业审计的对象可以是单个系统，也可以是一组系统。对以下三类业务系统应优先进行专业审计：一是承担业务工作相对比较重要的业务系统；二是在开发过程中存在问题比较多的业务系统；三是将要进行升级改造、数据迁移和整合的业务系统。

信息系统专业审计内容不仅是信息系统本身，还涵盖信息系统的技术文档、业务流程、岗位职责、数据质量、系统功能、系统接口、软硬件及整体绩效等。具体审计以下几方面内容：一是技术文档是否合规、完整、一致、可用；二是业务流程和岗位职责是否合规、是否存在安全隐患；三是系统数据是否规范、可用，基础数据是否统一；四是系统功能是否与技术文档一致、执行有效；五是系统接口是否规范、需求明确、设计正确；六是应用系统硬件设备效率及整体绩效是否明显。

3.3 审计依据、方法和工具

信息系统专业审计过程需严格遵照国家、北京市及相关行业领域信息化建设相关标准和准则，如参照《GB/T 8567-2006 计算机软件文档编制规范》进行技术文档合规性审核；参照《GB/T 19488.1-2004 电子政务数据元 第一部分：设计和管理规范》进行数据元素梳理分析；参照《GB/T 19487-2004 电子政务业务流程设计方法通用规范》进行业务流程梳理和业务建模等。

在审计方法上，综合采用多种方法实施审计。例如，通过开发商调研、质询和系统确认，审计技术文档与系统的一致性；通过参照《GB/T 8567-2006 计算机软件文档编制规范》分解的 273 项审计指标，审计文档的完整性、合规性；按照《GB/T 19487-2004 电子政务业务流程设计方法通用规范》执行一体化业务建模，审计业务流程和岗位职责的合规性；按照《GB/T 19488.1-2004 电子政务数据元 第一部分：设计和管理规范》进行基础数据分析与抽取，审计系统数据的可用性和规范程度；通过对系统接口进行在线监听和传输包分析，理清接口关系，审计接口的合理性和有序性；通过考察 CPU 使用效率、机房总体能耗与系统运行的能耗比，审计系统设备运行效率和能耗等。

为了提高审计的质量和效率，可综合采用各类定制、通用或开源的计算机辅助工具实施审计。例如，运用专业业务建模工具（如 HDBMW）构建基于 GB/T 18487 的全程一体化业务建模，产生业务构成的组成结构树、职责执行流程图、业务协作流程图和数据关系图的“一树三图”模型；运用数据元素设计工具（如 HDELEMENT）进行数据元素分析，排除噪声数据干扰，分析 U/C 矩阵，产生财政主数据；运用数据库开发工具（如 PL/SQL）对测试环境数据库的实例数据进行分析和确认，把握数据流转情况；运用数据库设计工具（如 PowerDesginer）实现数据库的 ER（Entity Relationship Diagram，实体关系图）模型分析和数据物理建模；运用开源的接口分析工具对网络接口如 Web 服务、Socket、Http 等接口进行在线监听和传输包分析。

3.4 审计组织保障

由于信息系统专业审计涉及信息系统的方方面面，因此需要由专业审计机构、审计业主单位、所审系统开发单位三方共同协作完成，缺一不可。

专业审计机构须具备从事专业审计所需的完备的专业技术能力和成熟规范的专业审计工作模式，且审计涉及的业务系统的开发单位、监理单位、咨询单位均不得承担该系统的专业审计工作；审计业主单位需派出专门人员指导审计机构的专业审计工作，并协调系统开发商组织召开系统文档介绍、系统演示等会议；所审系统开发单位需指定了解所审系统的项目经理或技术总监全程配合专业审计工

作，积极配合审计机构做好系统文档介绍和系统演示，保质保量地补充所缺失的技术文档，对审计机构提出的技术文档相关问题给予清晰明确的回答。

3.5 审计实施策略

按照被审计业务系统的复杂性、规模和开发商配合程度，将审计执行流程划分为以下三种：一是简易审计流程，适用于系统复杂程度不高、规模不大、资料齐全、应用情况良好、开发商紧密配合的应用系统的审计，这种情况下只需依托技术文档和开发商执行审计；二是一般审计流程，适用于系统复杂程度较高、规模较大、资料存在一定缺陷、应用情况良好、开发商紧密配合的系统的审计，这种情况下除了借助文档和开发商以外，还需要搭建测试环境进行审计；三是复杂审计流程，适用于系统复杂程度高、规模大、资料不全，开发商不配合的系统，这时要利用审计辅助工具，通过逆向建模分析，完成审计工作。

3.6 审计流程

信息系统专业审计主要分为前期准备、形式审计、实质审计、报告编制四个阶段实施。

1）前期准备阶段

审计机构收集审计对象系统的技术文档，并按照《GB/T 8567-2006 计算机软件文档编制规范》规范整理归类，形成13类技术文档的“技术文档清单”；按照《GB/T 8567-2006 计算机软件文档编制规范》分解审计指标，形成“审计指标模板”，保证审计工作有据可依；同时下发“开发商调研表”，包括功能调研表、接口调研表、报表调研表，掌握当前系统基本情况。

2）形式审计阶段

审计机构按照审计指标，对业务系统的13类技术文档进行逐项审计和评价，形成“审计指标表”；在指标审计基础上，从技术文档的完整性、一致性、可用性三个方面，对业务系统的技术文档分别给出形式审计结论，形成“审计结论表”。

3）实质审计阶段

审计机构首先以会议和面谈形式进行开发商质询，由开发商进行系统演示和讲解，审计机构在开发商的配合下，对业务系统的业务流、数据流、接口等逐一进行确认，并就审计中发现的问题与其进行沟通；其次，基于开发商调研表和质询反馈的情况，对技术文档与业务系统的一致性进行审计，包括操作功能、统计报表、系统接口、业务数据与文档一致性；最后，根据审计情况，对开发商提出文档补齐要求，系统开发商按要求对技术文档进行大规模内容补充。

4）报告编制阶段

补充文档是最终编制审核报告的重要依据和素材。补充文档主要包括五类：第一类补充文档是业务模型。开发商需在审计机构的指导下，按照《GB/T 19487-2004 电子政务业务流程设计规范》，采用“全程一体化精细建模”方法，建立组织模型、业务协作流程模型、职责执行模型和数据关系模型。其中最为核心的是业务协作流程模型，即指岗位职责之间的协作关系流程的模型，描述了表单流转路径，以及系统间接口和人机交互的协作关系。基于业务协作流程，可以实现组织组成、数据资源和职责的聚集与展现，形成上下贯通的一体化业务视图模型。

第二类补充文档是主要功能的页面交互设计。对常用功能操作界面进行整理，补充页面迁移图（图2）和说明、页面设计、页面（初始化、控件事件）数据流表以及关联字典等基础数据。

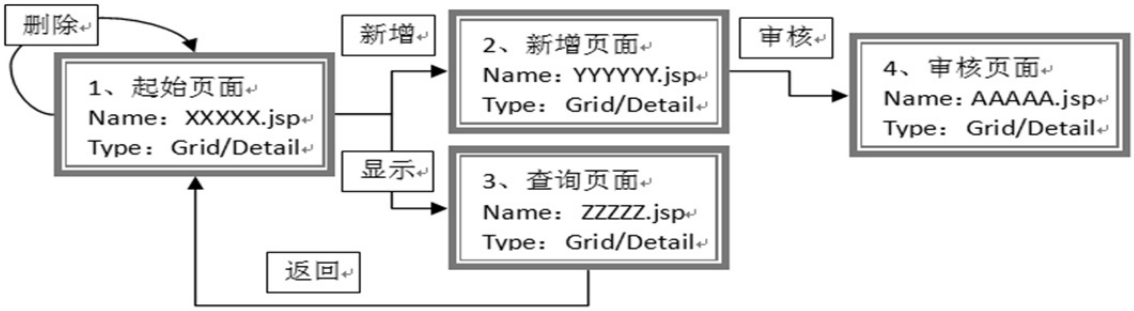

图 2　页面迁移图示例

第三类补充文档是报表设计。对报表的展示界面进行整理，补充报表页面、数据流和统计计算关系（图 3）。

```
REATE OR REPLACE FUNCTION FN_APP_DB_OUT_2010(↓
                                    --从支出总表取支出预算总表  JXY 2007↓
                                    OBJECT_CODE IN VARCHAR2, --采集对象↓
                                    ZXFS0        IN VARCHAR2, --展现方式↓
                                    AgencyCode0        IN VARCHAR2, --单位代码↓
                                    ObjectClass0        IN VARCHAR2, --科目_类↓
                                    ObjectTerms0        IN VARCHAR2, --科目_款↓
                                    ObjectItem0        IN VARCHAR2 --科目_项↓
                                    ) RETURN TYPES.CURSORTYPES IS↓
  RESULT        TYPES.CURSORTYPES;↓
  OBJECT_CODE0 VARCHAR2(30) := OBJECT_CODE;↓
BEGIN↓
  IF OBJECT_CODE0 IS NULL THEN↓
    OPEN RESULT FOR↓
      SELECT " OBJECT_CODE,↵
```

图 3　报表 PL/SQL 举例

第四类补充文档是系统接口，补充系统接口的整体结构，以及每个接口的业务描述（图 4）、接口类型、消息数据格式设计（图 5）、交换数据与业务数据表关系表。

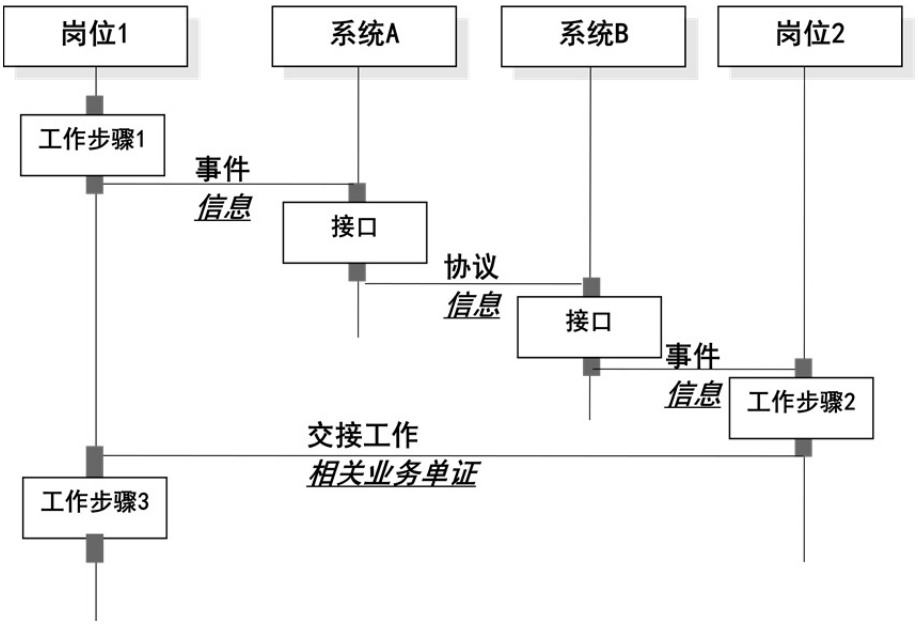

图 4 接口业务描述模板

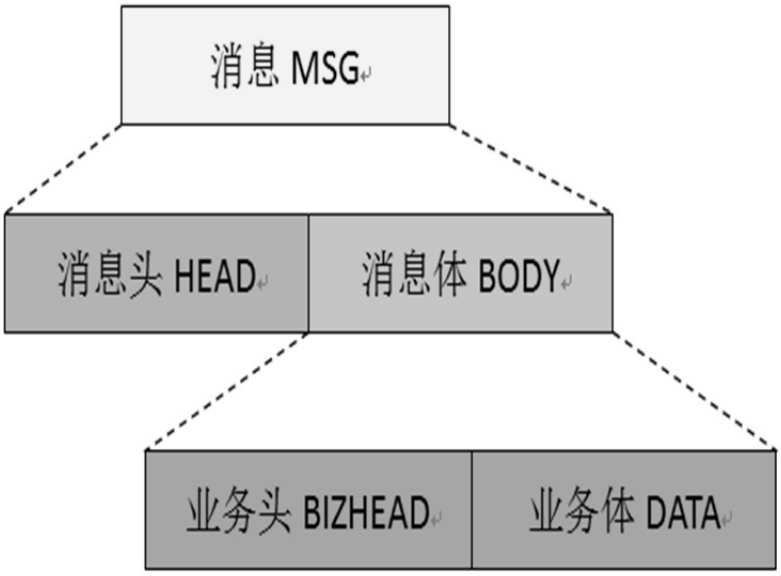

图 5 消息数据格式设计模板

第五类补充文档是对数据库字段的中文语义进行追加补充。

最后，基于前期审计过程编制审计报告。

3.7 审计报告

审计报告包括主报告和专项报告。主报告主要介绍审计工作的背景与目标、实施内容与过程、取得的成果、存在的问题及建议等，最后给出审计的总体结论；专项报告针对各业务系统给出审计结论。

除了主报告和专项报告，审计报告还附有五个附件，是审计报告的核心和精髓。附件一是“业务系统数据规则报告”，此报告是在开发商补充文档的基础上，由审计组进行审核确认，最终形成的对

业务系统数据规则的详细说明，内容包括系统的业务模型、交互页面操作数据规则、接口数据规则、报表数据规则等；二是“业务系统业务实体表编码”，描述系统内的全部具有中文语义的业务数据表，以及数据字典；三是“业务系统功能一致性审计状态表”，描述系统的功能、接口、统计数据现状，及其与文档的一致性审计评价；四是“业务系统技术文档审计指标表”，描述系统技术文档形式审计指标结论和说明。审计报告的展示方式是多样的，可以通过纸质方式存档，也可以开发专门的应用系统对成果进行展现和应用。

3.8 审计的作用

信息系统专业审计可以概括为对现有信息系统进行“摸底”和“改进”的过程。一方面，通过审计及时发现所审信息系统在技术文档、业务流程、岗位职责、数据质量、系统功能、系统接口、运维管理等方面存在的问题和不规范之处；另一方面，针对发现的问题，补充技术文档，对业务模型、系统功能、接口、数据关系等予以完善和修正，有效提升现有技术文档的可用性，保护了宝贵的历史数据资源，减少了对系统开发商的过度依赖，为今后系统进一步升级改造、数据迁移与共享交换奠定了基础。

4 信息系统专业审计典型案例

北京市某局在不同时期各业务部门按需建设的业务系统 89 个，在工作中发挥了重要作用，但由于应用系统在不同时期由不同厂商建设，开发架构、数据格式、技术标准不统一，难以满足未来该局业务协同、信息共享的需求。为了有效整治系统“乱”象，该局聘请第三方专业审计机构，对其 28 个核心业务系统进行了专业审计。

按照被审计系统的重要性，将 28 个系统分成二期、五个批次进行审计。通过前期调研了解到，大多数被审系统应用情况良好，开发商较为配合，且技术文档比较完整，仅有 1 个系统的技术文档完全缺失，开发商无法配合。因此审计项目组决定采用一般审计流程对其中 20 个系统进行审计，对 1 个系统执行复杂审计流程。审计过程中，审计业主单位派出 2 名专门人员指导审计机构的专业审计工作，8 家所审系统开发商指定了解所审系统的项目经理或技术总监共 13 人全程配合专业审计工作。本次审计历时 1 年，取得了良好的效果，具体如下。

一是技术文档的可用性显著提升。通过审计，找出该局 28 个核心业务系统在技术文档、业务流程、岗位职责、数据质量、功能接口、运维管理等方面存在的诸多问题，并针对审计发现的问题，补充技术文档，完善了系统业务流程，纠正了数据错误，理清了接口关系，共补充技术文档 4 852 页，其中业务协作流程 142 个，职责执行流程 1 116 个，交互界面设计 865 个，系统间接口关系 113 个，查询和报表 617 个，业务实体表单 1521 个，数据项 27 972 个。通过专业审计，技术文档的可用性达到 90%以上。

二是实现了项目管理系统优化整合。在审计之前，该局先后开发了市级项目管理系统、区县项目管理系统、文化创意产业项目库系统、中外合作项目库系统等 20 余个项目管理系统，各系统功能大量重复。通过审计，全面梳理了现有各类项目管理业务流程和管理方式，整合优化出一套适合各类项目管理的通用业务模式。将该局原有的针对不同项目开发的 20 余个项目管理系统整合归并为一套统一、通用的项目管理系统，减少了重复投资、重复建设。

三是运维和升级改造费用大幅降低，运维管理更加规范。在审计之前，该局由于存量系统多而杂，不得不过度依赖开发商，驻场开发商多达 100 余人，系统运维费用高居不下。通过审计，建立了一套基于国标的技术文档验收标准，从由不同开发商多头运维转变为统一运维，增强了政府部门对其信

息化建设的把控能力，减少了对开发商的过度依赖，运维费用也大幅下降。

四是为后续系统整合和数据迁移打下良好基础。通过专业审计，理清了该局业务主线，梳理“1 条核心业务线-25 个业务分类-147 项业务流程”的三级业务体系，形成业务全景图；基于业务线和业务分类，梳理跨系统的共享数据关系，初步建立基础数据标准，提升了数据标准化规范化程度，为后续政府部门信息系统一体化整合、数据迁移及后续系统开发奠定了坚实基础。

5 结论

上述理论研究和实践应用表明，本文提出的“信息系统专业审计”体系框架和方法对于解决系统与实际业务流程不匹配、信息共享难、系统与技术文档“两层皮”等方面的问题是有效的，虽然仍有很多需要完善的地方，但可以预见其所具有的十分重要的理论意义和广阔的应用前景。

参 考 文 献

[1] 胡克谨，等. IT 审计[M]. 第二版. 北京：电子工业出版社，2004.
[2] ISACA. IT Standards，Guidelines，and Tools and Techniques for Audit and Assurance and Control Professionals[S]. 2010.
[3] ISACA. Case study on using COBIT 5 for strategy implementation[S]. 2013.
[4] Weber R. Information System Control and Audit[M]. Upper Saddle River：Prentice Hall，1999.
[5] 庄明来，吴沁红，李俊. 信息系统审计内容与方法[M]. 北京：中国时代经济出版社，2008：22-23.
[6] 熊耀亮. 基于 COBIT 信息系统审计研究[J]. 科技信息，2012，（18）：269-270.
[7] 潘晓江. 电子计算机审计与数据可靠性控制[J]. 会计研究，1983，（5）：55-59.
[8] 唐清亮. 试论电算系统的审计[J]. 财经研究，1987，（4）：42-45.
[9] 张静，余建坤，尹建业，等. 国内外信息系统审计操作指南对比研究[J]. 全国商情：经济理论研究，2011，（Z3）：14-16.
[10] 李春青，周座. “国外引进”还是“自主发展”？——对我国政府信息系统审计发展途径的探讨[J]. 南京审计学院学报，2012，（1）：51-57.
[11] 王会金. 论信息系统审计准则在我国的需求与发展[J]. 南京审计学院学报，2012，9（6）：1-7.
[12] 刘杰. 我国信息系统审计准则构建研究[J]. 财会月刊，2014，（17）：43-47.
[13] 陈义生. 信息系统审计初探实例[J]. 审计与理财，2013，（5）：15-16.
[14] 张鹏，王延章. 信息系统审计在电子政务中的应用[J]. 中国管理信息化，2006，26（10）：47-49.
[15] 史达，张萍. 电子政务信息系统审计中的风险分析[J]. 电子政务，2008，（1）：38-43.

Theoretical Research and Practical Application on Information System Professional Auditing

MU Yong[1] ，ZHAO Ying[1] ，ZHANG Yansheng[2] ，ZHI Junhui[2]
（1. Beijing Information Resource Management Center，Beijing 100101，China；
2. Space Century Consulting Company，Beijing 100048，China）

Abstract In order to solve some common problems of many information systems in use，such as the system workflows not match actual business process，data not standard，hard for information sharing，system not meet the technical document，ect，the paper innovatively put forward the concept of “Information System Professional Auditing”，defines its connotation and extension，points out its objectives，targets，contents，basis，methods，tools，strategies，organization，process，result and effect. The theory has been practiced on 28 information systems in a government department，and got good results.

Key words information system professional auditing，research，practice

作者简介

穆勇（1965—），男，博士，高级工程师，北京市信息资源管理中心副主任，长期从事信息资源管理研究，参加和主持数字奥运、智慧北京多项政府信息化重大工程。E-mail：muy@bjeit.gov.cn。

赵莹（1984—），女，工程师，北京市信息资源管理中心项目主管。研究方向包括政务信息资源管理研究、政务大数据应用研究等。E-mail：zhaoy@bjeit.gov.cn。

张燕生（1957—），男，高级工程师，研究方向包括信息系统专业分析、软件开发架构分析等。E-mail：zhangyangsheng@huadi.com.cn。

支俊辉（1972—），男，高级项目经理，研究方向包括信息化咨询等。E-mail：zhijh@httz.cc。