GXXSA

GUOWAIXINXIXITONGSHENJIANLI

● 主编 钱啸森 ● 副主编 郭静 曾嵘

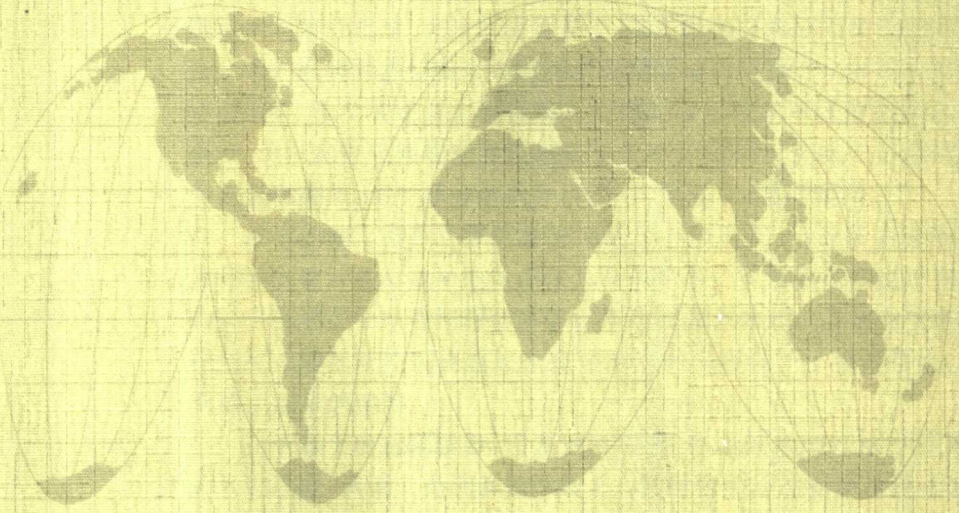
# 国外信息系统审计案例

中国时代经济出版社
China Modern Economic Publishing House

GUOWAIXINXIXITONGSHENJIANLI

● 主编 钱啸森 ● 副主编 郭静 肖峻

# 国外信息系统审计案例



中国时代经济出版社
China Modern Economic Publishing House

**图书在版编目(CIP)数据**

国外信息系统审计案例/钱啸森主编. —北京：中国时代经济出版社，2007.1

ISBN 7-80221-164-6

Ⅰ.国… Ⅱ.钱… Ⅲ.信息系统-审计-案例-国外 Ⅳ.F239.6

中国版本图书馆 CIP 数据核字(2006)第 101517 号

国外信息系统审计案例

主编 钱啸森

副主编 郭静 曾嵘

| | |
|---|---|
| 出 版 者 | 中国时代经济出版社 |
| 地 址 | 北京东城区东四十条 24 号<br>青蓝大厦 11 层 |
| 邮政编码 | 100007 |
| 电 话 | (010)68320825(发行部)<br>(010)88361317(邮购) |
| 传 真 | (010)68320634 |
| 发 行 | 各地新华书店 |
| 印 刷 | 北京市优美印刷有限责任公司 |
| 开 本 | 787×1092 1/16 |
| 版 次 | 2007 年 1 月第 1 版 |
| 印 次 | 2007 年 1 月第 1 次印刷 |
| 印 张 | 22.75 |
| 字 数 | 433 千字 |
| 印 数 | 1～5000 册 |
| 定 价 | 40.00 元 |
| 书 号 | ISBN 7-80221-164-6/F·039 |

# 序

会计是一种专业的商用语言，输出这种语言的是会计信息系统。

管理，随领域的不同，也形成了多种专业语言，输出这些语言的是各种不同功能的管理信息系统。

在手工条件下，会计信息系统主要由纸张和文字等要素构成的复式簿记系统组成。管理信息系统虽功能不同，但要素亦然。

千百年来，人们习惯于在手工条件下输入、加工、输出和使用会计语言和管理语言，同时也在不断地改进形成这些语言的会计信息系统和管理信息系统。

然而，一种由计算机技术、网络技术和通讯技术组成的信息技术出现在上世纪，并在上世纪末和本世纪初获得了飞速发展。它的出现和发展打乱了人们的传统习惯，甚至改变着人们的思维方式，对人们的生产和生活带来了巨大的影响。对于审计而言，情形完全相同。

应该承认，信息技术的出现，改变了会计信息系统和管理信息系统的构成要素，给人们带来效率和质量的同时，也给审计带来了挑战。在手工系统条件下，当手工数据发生问题或产生异常时，审计人员可以非常方便和简单地对系统进行处理或更正，甚至可以事先对系统进行审查。但是，在所谓电子系统或信息化环境下，当电子数据发生问题或产生异常时，审计人员可能完全无能为力，而且不可能对系统有所作为。

古人讲:物有本末,事有始终,知所先后,则近道矣。其本乱而末治者否矣。几乎可以肯定地讲,系统有问题而数据无问题的情况是十分罕见的。要想取得真实、完整和有效的数据,就应该首先对系统有所作为。如果不能事先对系统进行审查,发现数据异常时对系统又无能为力,那是审计人员的悲哀。因此,作为称职的审计人员,无论如何也要破解这个难题。

好在系统由传统转变为现代的同时,审计人员也在实现这种转变。为了解决本末问题,自上世纪后期至今,世界上许多国家的审计人员和计算机技术人员,对信息系统审计进行了不懈的探索,也确实取得一些有用成果。在我国,信息系统审计也开始蹒跚起步。

应该讲,在信息系统审计起步阶段,对于多数审计人员而言,主要的任务还是学习,也需要在实践中不断摸索。在这个过程中,间接经验更显宝贵。我感觉,本书的编写、编译和出版可以起到为广大审计人员提供间接经验的作用,这可能也是本书译著者的初衷。

学习国内外的间接经验可以帮助我们提高认识,少走弯路,节约资源。粗读本书,感觉它确实有助于达到此目的。

本书并非饕餮大餐,但也十分精道。既有案例,又有准则、指南和程序,还有一些模拟试题。细心读来,肯定大有裨益。

为人做序者,必精所序书中之道,然而我却在门外。为了表达与译者相同的想法,与读者一起学习信息系统审计,并尽快登堂入室,斗胆为序。

石爱中

2006 年 8 月 15 日

# 前　言

进入21世纪，我国审计工作步入快速发展时期，社会信息化程度也在不断提高，我们正逐步向信息化社会迈进。信息系统也广泛深入地渗透到社会的各个领域，成为政治、经济、军事、文化乃至社会一切领域的基础，也使得信息系统审计这一课题日益引起人们的关注。

信息系统审计(Information Systems Audit，简称IS审计)也称为IT审计，是对信息系统的规划、开发、运行和维护等各个环节进行评价，确保其符合其经营管理目标的过程。20世纪90年代以来，随着以计算机和网络为特征的信息系统的普及，信息系统审计应运而生，它最早出现于美国。IS审计作为信息社会的安全对策，能有效地管理与信息系统相关的风险，从而确保信息系统的安全性、可靠性和有效性。我们相信，在未来的几十年内，中国的信息系统审计必将会有一个很大的发展，且在我国信息化进程中具有重大战略意义。

目前，全国政府审计人员、内部审计人员、注册会计师以及广大社会人员，学习信息系统审计的热情非常高，大家都希望得到一些思路、多学习一些技术、尽快打开信息系统审计的局面。考虑到我国开展各种现代审计的时间较短，虽然在信息系统审计方面开展了多种形式的探索和尝试，但尚处于不太成熟的阶段，没有总结出比较系统的技术和方法。在这种情况下，学习借鉴国外信息系统审计的成功经验，洋为中用，不仅有利于我们对问题的认识，而且可以使我们的信息系统审计理论研究与实践探索少走弯路，节省宝贵的时间和资源。

本书分为三个部分。第一部分的章节主要介绍国外信息系统审计各个层面的若干案例。第二部分的章节主要介绍信息系统审计准

则、指南和程序。第三部分的章节涉及国际注册信息系统审计师(Certified Information Systems Auditor,简称 CISA)考试,为有志考取 CISA 的读者提供了模拟试题和参考答案。

学习国外信息系统审计,关键在于学习其思路和方法。因此,本书第一部分特别汇编了包括澳大利亚、美国、加拿大等较早开展信息系统审计的国家经典案例。案例思路开阔、涉及面广,从信息系统审计的计划组织到技术构架,从信息安全保护到灾难恢复,从软件系统开发和获得到实施和维护,从信息系统的商业流程评估到风险管理等。这些案例从各个方面展示了如何对成熟的信息系统进行审计,并用通俗的语言对审计的方法和技术进行了阐述,这将有利于人们从科学的角度,了解和学习如何开展信息系统的监督、检查和审计,规避信息系统管理中的风险,提高信息系统安全的保障。

学习国外信息系统审计的经验,还要善于学习借鉴那些已经成形的程序、指南和标准。因此本书的第二部分特别介绍了信息系统审计的准则、指南和程序。其中包括国际最高审计组织的信息系统安全检查方法,计算机安全研究企业的信息安全管理审计检查清单,COBIT 框架。这些标准、指南和程序不仅为开展信息系统检查和审计提供了指导,也对信息系统设计者提供了有价值的工作参考和考核目标。

国际信息系统审计与控制协会(Information Systems Audit and Control Association,简称 ISACA)的总部设在美国,是 IT 治理、控制和保证的全球性专业协会,其一年一度举办的注册信息系统审计师(Certified Information Systems Auditor,简称 CISA)考试得到全球的广泛认可,考试合格并获得职业资格者可在全世界范围内开展信息系统审计工作。国际注册信息系统审计师已被认为是最具前景的十大职业之一。CISA 考试要求应试者既要精通审计和管理,又要掌握计算机信息技术。目前,信息系统审计师已经成为全世界范围内最抢手的高级人才。针对中国的广大考生缺乏中文复习资料这一状况,本书特别介绍了 CISA 考试并翻译了 150 道考试模拟题。

总之,本书较全面地反映了信息系统审计的各个层面,通过分析丰富的案例,既通俗易懂,又有很强的可操作性。本书的出版对促进

我国更好地进入信息社会，保障信息安全将起到积极的作用。希望通过本书的出版推进我国的信息系统审计工作，有助于培养国际注册信息系统审计师队伍，促进信息系统更加安全、可靠与有效，从而为我国信息化建设做出一份贡献。也希望本书能够成为审计专业学生、对审计学科感兴趣者、有志了解和参加国际注册信息审计师考试者以及那些渴望成为信息系统审计专家的人员提供了有价值的参考资料。

**钱啸森**

2006 年 11 月于北京

contents 目录

序
前　言

第一部分　国外信息系统审计案例

一、信息系统计划组织与技术构架　3
【案例 1】澳大利亚审计署对退役军人事务部 IT 服务外包合同管理的审计　3
【案例 2】澳大利亚审计署对 Centrelink 信息技术管理的审计　11
【案例 3】澳大利亚联邦政府互联网安全的审计　21

二、信息安全保护与灾难恢复　30
【案例 4】对加拿大多伦多市政府 ORACLE 数据库安全审计　30
【案例 5】TALLAHASSEE 市审计局对本市局域网进行的逻辑安全审计　36
【案例 6】美国审计署对联邦存款保险计算机病毒保护程序的审计　44
【案例 7】澳大利亚审计署关于政府中心网络商业永续和危机管理的审计　49

三、运用软件系统开发、获得、实施及维护　61
【案例 8】对加拿大电子通用信息管理系统（eCIMS）开发的审计　61
【案例 9】美国审计署对联邦存款保险公司时间和出勤处理系统开发项目审计　68
【案例 10】加拿大伯克利市审计局对该市财政系统变更的审计　74

contents

四、商业流程评估及风险管理与综合案例 82
【案例 11】对 GIAC 公司 Unix 系统的审计 82
【案例 12】美国审计署关于 SBA 财务管理信息安全的审计 97
【案例 13】澳大利亚卫生与老龄人口部信息技术审计 104
【案例 14】加拿大审计署对政府信息技术安全的审计 113

第二部分 信息系统审计准则、指南和程序

一、美国信息系统审计与控制协会（ISACA）的信息系统审计准则、指南和程序摘要 123

二、国际最高审计组织的信息系统安全检查方法 187
——对政府机构信息系统安全进行检查指南

三、美国系统网络安全协会（SANS）信息安全管理审计检查（清单） 229

四、美国信息系统审计与控制协会（ISACA）的 COBIT 框架简介 252

第三部分 国际注册信息系统审计师（简称 CISA）考试及模拟题

一、国际注册信息系统审计师 289
二、习题汇编 291
三、习题答案 319

# 第一部分

# 国外信息系统审计案例

# 一、信息系统计划组织与技术构架

## 【案例 1】 澳大利亚审计署对退役军人事务部 IT 服务外包合同管理的审计

### 背景

澳大利亚政府依赖退役军人事务部(The Department of Veterans' Affairs,以下简称 DVA)向退役军人及其家属提供支持性服务,包括赡养、战争赔偿、医疗费支付等等。如今,DVA 的服务对象已超过 500 万人。

DVA 是第一个外包 IT 服务的联邦政府部门。截至 1997 年 2 月,DVA 的服务外包涵盖了所有的底层技术平台,包括:

1. 大型主机系统维护,如商业永续管理,灾难恢复流程设计,服务器、数据库配置管理及能力规划,软件、网络、数据库日常维护支持;

2. 桌面系统支持,如系统软件、应用以及办公软件、打印、扫描、传真及相关局域网等各类问题的解决;

3. IT 运营环境支持,主要涉及底层技术、硬件(服务器和存储设备)、数据安全、语音通信和办公自动化服务。

IBM 澳大利亚有限公司(简称 IBMA)承揽了 DVA 所有底层技术服务,提供系统安装、现场支持、零部件修理与更换、程序修正与升级。合同于 1997 年 2 月签订,总价值 6500 万美金,期限 5 年。概括地说,DVA 希望从该 IT 服务外包合同中获取如下收益:

1. 通过 5 年的 IT 服务外包,节省 200 万运营成本;

2. 采用更先进的底层技术支持 DVA 的对外服务,提高服务水平;辅助业务部门实现商业目标、提高绩效;

3. 为退役军人提供更优质的服务；

4. 为地方创造工作机会，促进中小企业的发展；

本次审计是澳大利亚审计署于 1999 年施行的。

## 审计目标

1. 确定 IT 服务外包合同与公司 IT 战略、商业目标的一致性；

2. 评估合同内容的充分性；

3. 评估合同管理流程的有效性。

## 审计范围

审计署全面审查了 DVA 的 IT 服务外包合同（又称为信息服务战略协议 Strategic Information Service Agreement，简称 SISA）的具体内容，了解了合同管理流程，评估合同执行成果。需要说明的是：本次审计不涉及招标流程的设计与管理。

## 审计方法

1. 通过审查文档，掌握合同管理流程，分析合同内容，了解付款过程；

2. 与部门经理以及关键员工面谈；

3. 在 DVA 总部和几个地方机构进行现场调查，搜集数据。

审计署雇佣了一家专门从事 IT 合同管理研究的法律咨询公司，针对如何保护联邦政府利益的问题，审查合同内容并提出合理建议。

## 基本审计结论

DVA 以确保 IT 服务不间断交付为核心目标，对服务外包合同实施了有效管理。然而，本次审计也发现了一些战略层面和操作层面的问题，期待 DVA 在以后的工作中改善提高，包括：

1. IT 战略计划与服务外包合同的内容缺乏一致性，广泛应用的客户机—服务器技术没有在合同中予以体现，更没有纳入服务范围；

2. 缺乏足够的数据以评估合同执行情况；

3. 合同在某些重要方面的阐述不够明晰。比如，服务内容、服务等级的定义不够明确；拟定的服务标准没能反映出业务需求；没有把风险评估纳入合同管理流程。

## 审计的主要发现

### 一、IT 服务外包合同满足战略需求

**● 战略一致性**

IT 服务外包应符合并有助于实现机构整体战略，预见 IT 未来的发展，考虑潜在的机遇与风险、收益与成本。DVA 已经成立了一系列 IT 委员会以支持、辅助业务运营，将 IT 服务管理与核心业务相融合。

**● 满足商业需求**

IT 服务外包要基于明确的商业需求，保证合同内容与需求的一致性，并建立一个合理的、有成本效益的改变管理流程应对需求的变化。同时，尽可能地预见未来需求，洞悉信息技术的发展。然而，DVA 的现行合同要求合同条款包括服务等级在 5 年有效期内维持不变，对于 IT 这样一个日新月异的行业来说，执行起来非常困难。建议 DVA 定期和供应商就合同内容以及价格进行磋商，考虑潜在的需求、技术的发展趋势，将其纳入合同。

**● 服务外包的方式**

DVA 仅指定了主供应商，授权该主供应商选择子供应商。这种方式使得 DVA 只面对一个供应商，避免了用于管理、协调多个供应商的费用，降低了交易成本。

**● 与计划内需要的一致性**

1. DVA 没有将日益广泛应用的客户机－服务器技术纳入合同范围。

2. 1999 年至 2000 年期间，DVA 进行了 8 项政策修订。相应地，IT 系统需做出重大调整以支持新政策。为应对某些难于遇见的政策调整，DVA 必须提高 IT 系统的弹性与处理能力。

3. DVA 的现行合同没有涉及附加需求，而是将其作为一种附属物单独处理，继而带来了额外成本。审计署建议 DVA 将附加需求和基本需求作为一个整体考虑，并纳入合同范围。

**● 适应需求的变化**

外包合同执行期间，DVA 对 IT 系统的处理能力、存储能力、性能的要求都有了较大提高，主机系统的负载已增长了近 4 倍，服务器数量已从 34 台增长至 130 台。这种压力很可能带来财务问题，并造成 IT 服务质量的降低。1998 年 DVA 进行了两次合同变更以反映这种高利用率。DVA 应与供应商进一步磋商，认真考虑应对措施。

## 二、合同内容

### ● 交付物与服务标准

1. 有些交付物在合同中定义不够明晰，使得 DVA 难于确保供应商交付的服务是否完全，质量是否达标。

2. 没能将业务需求转化为 IT 系统需求，清晰地建立彼此之间的关联，因此很难确保合同规定的交付物、响应时间恰当地支持业务运营。如果这一状况得不到改善，随着业务需求的变化与增长，合同内容偏离业务运作的风险将日益扩大。

3. DVA 在 2000 年对 IT 外包合同的执行情况进行了审查，发现了一些重要的未交付或仅实现部分交付的服务，包括灾难恢复计划、IT 人员操作技能培训、IT 系统性能跟踪以及年度财务报告。为解决这些问题，DVA 要求供应商每 6 个月进行一次客户满意度调查，从最终操作人员的角度评估服务的质量，排列服务的优先级。根据调查结果，更新需求，重新议定合同价值，排除不必要的服务。审计署对 DVA 采取的这项措施表示认同。

4. 建议合同约定的服务标准适用于所有底层技术。

### ● 相关问题

1. 许可软件

合同规定：供应商有权提供服务所需的第三方软件。但是，现行合同的条款不能保证软件价格的公平性。建议：在今后拟定合同时，明确指出这类许可软件的价格应不高于市场价值。

2. 甲方(联邦政府机构)的责任义务

SISA 没有区分合同涉及的 3 个联邦政府机构各自的责任义务。为此，三方单独拟定了一份契约书，以协调对合同的管理。但是，该文档内容不够全面，比如没有明确指出任何一方中途退出协议所造成的影响、给其他政府机构带来的额外费用。

3. 保密

IT 外包合同要求供应商的员工、代理人及其雇佣的子包商签订保密协议，并遵守 DVA 的各项信息技术安全规定。为避免数据被窃取，禁止供应商将用于 DVA 数据处理的大型主机共享，以处理其他客户的业务。DVA 同意将包含客户信息的磁带采用自动的方式导入供应商的大型主机系统，同时要求供应商担保该数据的机密性。但是，审计署发现，DVA 没有审查供应商实际采用的数据转移过程，也没有采取监控措施。

4. 合同条款的机密性

DVA 规定不得将本协议内容向第三方或公众透露，仅 DVA 内部相关员工有权访问该合同副本。协议中有关服务提供方式、服务内容等非机密

信息将在DVA内部局域网上发布，供员工共享。但与服务费用相关的资料属机密信息，受到保护。

这种约束将妨碍DVA员工对合同条款的理解、对合同执行的管理。另外，参议院曾反复重申："除非有正当理由，合同信息应对公众公开"。审计署也指出："国会及所属委员会有权访问合同内容"。考虑到这些要求，DVA在续签合同时，需重新考虑保密条款。

5. 合同访问权

为履行合同管理义务，评估供应商绩效，合同规定：允许DVA一方的合同经理或其授权人员以及内部审计人员访问合同内容、执行记录。另外，如果DVA需要，供应商应参与DVA对IT系统的审计。

6. 续约与服务移交

i. 合同规定：甲乙双方均有权对是否续签合同提出建议。一方提出申请4周内，对方应给与回复。如果供应商没能履行合同内容，提供满意服务，DVA有权终止合同。续期合同有效期为2年。如果DVA希望合同续延少于2年，则需双方协商认可。审计署对此规定没有异议。

ii. 目前，DVA没有文档明确定义：在服务转移的过渡时期，供应商应有的人员投入、技术投入。

iii. 现行合同没有要求供应商提交详细的流程操作手册和设备使用列表。如果DVA终止与IBM的合作，这将给其他供应商接手工作造成困难，更给DVA带来风险。

## 三、合同管理

### ● 风险管理

风审计署将IT服务外包所涉及的风险划分为3种类型：

1. 运营风险

DVA运用商业永续计划来管理运营风险，其中定义了关键业务操作，并指定了重要性等级。灾难发生时，DVA将根据其重要性，顺序恢复各业务操作。

通过抽查，审计署认为DVA的商业永续计划指出了IT服务中断所带来的潜在运营风险，总体上恰当有效。但是，这些文档均依赖于供应商负责提供的《灾难预防措施》和《灾难恢复流程》。

2. 与供应商提供服务相关的合同风险

i. 尽管商业永续计划草案在1998年中期就已拟定，但是直至2001年也没有最终生效。这有悖于合同规定，致使供应商的《灾难恢复流程与行动计划》迟迟没能完成。

ii. 商业永续计划指出《灾难恢复流程与行动计划》需测试以验证其有效