内部控制丛书

计算机信息系统控制与审计

张金城 著

NEIBU KONGZHI CONGSHU

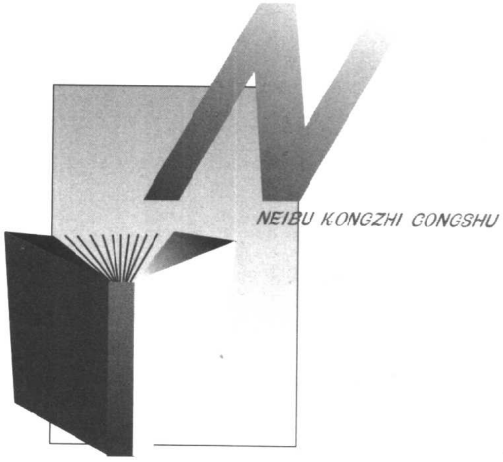
北京大学出版社

江苏省青蓝工程基金项目

内部控制丛书

计算机信息系统控制与审计

张金城 著



北京大学出版社

图书在版编目(CIP)数据

计算机信息系统控制与审计/张金城著. —北京:北京大学出版社,2002.4
ISBN 7-301-05046-1

Ⅰ.计… Ⅱ.张… Ⅲ.计算机应用—审计 Ⅳ.F239.1

中国版本图书馆 CIP 数据核字(2001)第 034699 号

书　　名:计算机信息系统控制与审计
著作责任者:张金城　著
责任编辑:林君秀　王煜玲
标准书号:ISBN 7-301-05046-1/F·0423
出 版 者:北京大学出版社
地　　址:北京市海淀区中关村北京大学校内　100871
电　　话:出版部 62754962　发行部 62754140　编辑部 62752027
排 版 者:北京华伦图文制作中心 82871385
印 刷 者:北京大学印刷厂
发 行 者:北京大学出版社
经 销 者:新华书店
787×980 毫米　16 开本　22 印张　368 千字
2002 年 4 月第 1 版　2002 年 4 月第 1 次印刷
定　　价:38.00 元

内容提要

本书全面系统地论述了计算机信息系统控制与审计的基本知识、基本理论、基本方法与技术。本书的特点是既注重系统性和科学性，又注重实用性；既有原理性论述，又有丰富的实例与之配合。本书共分十四章。第一章和第二章论述了计算机信息系统及其控制与审计的基本知识；第三章至第七章分别论述了计算机信息系统各要素的审计方法；第八章和第九章论述了计算机辅助审计信息系统的开发方法，并通过实例说明如何开发审计软件；第十章至第十三章论述了高级的计算机信息系统控制与审计方法；第十四章论述了计算机犯罪的控制与审计方法。本书是江苏省青蓝工程基金项目成果。本书可作为管理类相关专业本科生或研究生的教材和教学参考书，也可供广大审计人员、信息系统开发及管理人员学习、参考。

作者简介

张金城，男，南京审计学院管理学系副主任、教授，江苏省跨世纪学术带头人，东南大学经济管理学院在读博士。从1988年起，在会计、审计等类杂志上公开发表会计电算化、管理信息系统、计算机信息系统审计等方面的论文50余篇，出版专著4本，有多篇论文(著)获奖，曾为大中型企业开发多套财务及管理软件。

前　言

在计算机技术日新月异，信息系统电算化日益普及的年代里，作为一名审计工作者，掌握计算机信息系统的控制与审计的原理和方法，是十分迫切的，也是完全必要的。

为适应我国审计形势发展的迫切需要，作者编写了这本《计算机信息系统控制与审计》。本书在写作过程中，注意吸收和参考先进国家计算机信息系统控制与审计的基本理论和技术方法，并结合我国计算机应用与计算机审计发展的实际情况和作者多年的研究成果，在内容上力求兼顾先进性和实用性，做到理论、方法与应用有机结合，有较强的可操作性。

本书共分十四章。第一章论述了计算机信息系统控制与审计的基本知识，使读者能对计算机信息系统的控制与审计有一个概括性的了解；第二章论述了计算机信息系统的基本知识，使读者对计算机信息系统有一定的了解，以便阅读以后各章；第三章、第四章论述了计算机信息系统一般控制和应用控制及其审计方法；第五章、第六章、第七章、第十章、第十一章、第十二章、第十三章、第十四章系统地论述了系统开发、应用程序、数据文件、联机信息系统、终端机作业、数据库系统、计算机网络信息系统、计算机犯罪的控制与审计方法和技术；第八章、第九章论述了计算机辅助审计信息系统的开发方法，并通过实例说明了如何开发审计软件。

本书对广大审计人员进行计算机信息系统审计，对计算机信息系统管理人员探讨加强计算机信息系统的控制，对计算机工作人员研究计算机在实际业务中的应用和控制，对审计、会计、管理、计算机等专业师生的教学与科研，都具有很高的参考价值。

本书在写作过程中，自始至终得到了南京审计学院院长易仁萍高级审计师、副院长李凤鸣教授、副院长乔春华教授的指导、关心与大力支持，在此表示衷心的感谢。

由于计算机信息技术突飞猛进，计算机信息系统控制与审计涉及的知识范围十分广泛，书中难免有错误与不当之处，恳请广大读者予以指正。

作　者

2002 年 4 月

目　录

第一章 概 论

第一节 计算机信息系统内部控制概述

一、信息系统电算化对传统内部控制的影响

(一) 手工信息系统中严格的凭证制度,在计算机信息系统中逐渐减少或消失

凭证是经济业务活动的依据,设计良好的凭证格式及其传递程序,具有较强的控制功能,一旦发生某些错弊,凭证就成为追查责任的根据。在计算机信息系统中,特别是在联机实时系统中,终端操作者经常把业务直接输入计算机,而没有留下任何凭证。例如,定货业务,定货者可以通过电话把业务直接输入系统,在这种情况下,如果没有适当的控制,未经授权批准的业务就可能进入系统,审计线索也可能消失。

(二) 传统的手工信息系统所具有的分工功能逐渐被归并

在手工信息系统中,职责划分是一项重要的内部控制制度。例如,在会计系统中,记录总账和记录明细账的职责要分工。但在计算机信息系统中,这些分工功能逐渐被并入电子数据处理系统中。例如,在工资处理系统中,计算机既记录所有职工的工资及其工资率,记录职工的工作时间,又计算职工每月的工资,打印职工的应发工资等等。

在计算机信息系统中,若采用非数据库处理系统,因每个个别的系统各自拥有的储存媒介,仍可核对两个由不同人员负责处理的系统所产生文件的内容而发现错弊的存在,尚可勉强维持职权划分的部分功能。例如,负责账务处理系统的人员,若无法接触应收账款系统,则其篡改客户的行为,必因核对两个系统产生的独立文件内相同资料项目而被发现。但当组织采用数据库管理系统时,因相同资料仅输入及保留一份在数据库内,各系统不再个别重复建立其本身使用的数据库,则上述非数据库系统所具有的职权划分的功能已不复存在。

(三) 计算机信息系统可以自动授权、批准

授权、批准控制是指各级业务人员必须获得授权和批准,才能执行某项业务。在传统的手工信息系统中,对于一项经济业务的每一个环节都要经过某些经授权的人员的签名或盖章。但在比较先进的计算机信息系统里,可直接由电子数据处理功能取得授权、批准。例如,业务经办人可以利用特殊的授权文件,如录有监督码的磁性识别卡,插入(或输入)机器内,即可获得批准终端机或运转有关的特定系统。这与手工信息系统只重视纸张文件上是否有签名或盖章的作业方式,显然不同。

在计算机信息系统中,计算机还可以自行产生一些业务处理。例如,系统设计员可根据存货控制理论,预先算好各种存货的经济订货量和再订货点,并把这些信息存储于系统中,系统就会监督存货定额,一旦存货低于再订货点,系统就会按经济订货量自动开出定货单,而没有具体人员的批准。

(四) 计算机信息系统的信息容易丢失、被盗窃和被篡改

在手工信息系统中,由于各项经济业务记录于书面纸张,是肉眼可见的,一般来说,不容易丢失。一些舞弊人员篡改账表单证的行为也会留下痕迹,这些痕迹是手工信息系统一项固有的控制措施。但在计算机信息系统中,各项经济业务存储于电、磁介质上,是肉眼不可见的,而且这些电、磁介质在受热、受潮或强的电磁场下都会损坏。因此,存于这些电、磁介质之上的信息有丢失和毁坏的危险。另外,在操作时,除了工作人员疏忽大意容易将存储于这些磁性介质之上的信息毁坏之外,如果没有适当的内部控制,一些舞弊人员还可进入系统,对存储于这些电、磁介质之上的信息以及对程序进行篡改或拷贝,而不留下任何痕迹。

(五) 电、磁介质存储数据缺乏证据力

在手工信息系统中,信息被记录于凭证、账簿等纸张上面,这些信息以纸作为载体,而在计算机信息系统中,则主要以磁盘、磁带等磁性介质作为信息的载体。从内部控制的角度看,电、磁介质有一个很大的弱点,即记录于磁性介质之上的信息缺乏证据力。这主要是因为:

(1) 利用电、磁介质很容易通过拷贝进行数据的复制,因而无法区分正本和副本;

(2) 记录于电、磁介质上的信息是肉眼不可见的,必须借助于计算机的"翻译"才能以肉眼可见的形式表现出来,但同一信息是可以"翻译"成不同形式的;

(3) 利用电、磁介质无法实现像签字、盖章这样的使信息证据化的

操作。

因此，如果单纯依赖电、磁介质这种信息载体，则可能造成责任不清、真伪难辨，使审计缺乏具有法律效力的证据。

（六）数据与责任高度集中

在手工信息系统中，许多资料分散保存在企业的各个责任部门，没有经过授权批准的人很难花很多的时间分别到各部门的文件柜里浏览所有的文件。但在计算机信息系统中，全部的数据高度集中于电子数据处理部门，如果没有适当的控制，未经授权批准的人可以轻而易举地利用指令来浏览所有的文件，一些机密数据也很可能被不法分子很方便地拷贝甚至可能被非法篡改而不留下任何痕迹。

除了数据高度集中外，计算机信息系统的另一风险就是责任高度集中。例如，在手工会计信息系统中，由经济业务产生原始凭证，根据原始凭证，编制记账凭证；根据记账凭证，登记账簿；根据账簿，编制报表。每一步都有文字记录，每一步都有经手人负责。但在计算机会计信息系统中，原始数据一经输入计算机，就由计算机按程序指令自动处理，无论是算账、报账，还是编制报表，全由计算机自动处理，中间一般没有经手人负责，全部责任都高度集中于电子数据处理系统。

（七）差错的反复发生

在手工信息系统中，发生差错往往是个别现象，而且由于数据处理各环节分散于多个部门，由多个人员完成，一个部门或人员的差错往往可以在下一个环节中被发现并被改正。由于计算机处理依靠程序运行并且运算速度极高，其处理结果一旦在某一环节发生错误，就能在短时间内迅速蔓延，使得相应的文件、账簿乃至整个系统的信息失真。如果错误是由于应用程序和系统软件造成的，则计算机会反复执行同一错误操作，多次给出错误结果。

（八）计算机信息系统的设计可能没有考虑审计的需要，没有留下充分的审计线索

审计线索在审计中是非常重要的。在手工信息系统中，审计人员可以从原始凭证开始，对业务进行追踪，一直到报表为止；也可以从最后的报表开始，追根寻源，一直追溯到原始凭证。对手工信息系统的审计，就是建立在这种肉眼可见的审计线索之上。但在计算机信息系统中，各类数据文件都存储在肉眼不可见的介质上，纸性材料大大减少。如果设计人员考虑不周的话，很可能设计出的系统没有留下充分的审计线索。如果出现这种情

况，不仅日后的审计难以进行，而且也为舞弊分子大开了方便之门。

二、计算机信息系统内部控制的目标

计算机信息系统内部控制的目标，是指通过控制所要解决的问题和所要达到的目的。可概括为以下六个方面：

（一）确保系统的合规合法

计算机信息系统与手工信息系统一样，系统本身及其所处理的经济业务必须符合国家有关的法律、法令、方针、政策，符合有关部门颁布的各种规章制度、条例等，如现行的会计制度、财务制度等。因此，在设计系统的过程中以及系统运行阶段，必须建立适当的内部控制，确保系统及其所处理的经济业务合规合法。

（二）保证系统处理的数据正确无误

保证系统处理的数据的正确性，是计算机信息系统内部控制的基本目标。为了保证系统处理数据的正确性，在系统设计过程中，要注意设计程序化控制，如平衡控制、合法性控制、总数核对控制、合理性检验、纠错系统检验、输入数据类型检验、顺序检验等。在系统运行过程中，要对数据输入环节进行严格的控制，确保输入数据的正确性。

（三）保证系统安全可靠

保证计算机信息系统的安全可靠，是系统能够正常运行的前提和基础。因此，在系统正式投入运行之前，就应考虑系统的安全性，通过建立严密完善的硬件、软件和数据安全措施，来保证系统的安全可靠。

（四）提高系统运行的效率

计算机信息系统的运行效率在很大程度上决定于输入数据的速度。因此，在系统输入设计环节，可采用适当的控制设计技术，提高系统输入的效率。例如，在计算机会计信息系统中，凭证编号由计算机自动生成，会计科目以编码的形式输入，规范摘要的格式，常用的摘要可用代码输入等。

（五）提高系统的可维护性

系统维护的工作不仅量大而且复杂。可维护性是指系统易理解、易修改和扩充。为了达到这一控制目标，从系统开发工作一开始，就应该考虑到今后的维护工作。在系统开发过程中，必须对系统开发的每一个环节进行严格的管理和控制。

（六）增强系统的可审性

所谓可审性，是指有能力、有资格的审计人员，能够在一个合理的时间

和人力限度内，对系统的正确性和可靠性等作出公正的评价。影响计算机信息系统可审性的因素较多，其中一个重要的因素就是审计线索。计算机信息系统的审计线索既容易被销毁，也容易被篡改，若设计时考虑不周，则很难进行事后审计。因此，只有在计算机信息系统的输入、处理和输出等设计环节采取适当的控制措施，例如：在计算机会计信息系统中设立总账、明细账、记账凭证等各种数据库，才能保留各种审计线索，才便于对会计数据的追踪审查。

三、计算机信息系统内部控制的分类

按照一定的标准对计算机信息系统的内部控制加以分类，有助于对其理解、审查与评价。

依据控制的范围，可分为一般控制和应用控制。一般控制指对计算机信息系统构成要素及其环境的控制。之所以称为“一般控制”，一方面是因为这些控制措施普遍适用于所有的计算机信息系统，另一方面是它们为每一个计算机信息系统的正常运行提供了安全可靠的环境。应用控制是针对具体的功能模块及业务数据处理过程各环节的控制。一般控制是应用控制的基础，应用控制是一般控制的深化。

依据控制的预定意图，可分为预防性控制、检查性控制和纠正性控制。预防性控制是为了防止错弊的发生而设置的控制；检查性控制是用来检查、发现已发生的错弊而设置的控制；纠正性控制是为了消除或减轻错弊事件造成的损失和影响而设置的控制。预防性控制是一种积极的控制，它试图在错弊发生之前加以防范，输入环节的控制大部分是预防性控制；检查性控制是一种中性控制，它试图在错弊发生的同时就能发现；纠正性控制是一种消极控制，它是假定错弊已经发生，设置一些可以减少错弊影响的手段。

依据控制所采取的工具或手段的不同，可分为手工控制和计算机程序控制。一般控制大部分是手工控制，应用控制大部分是程序化控制。由于计算机信息系统是一个人机系统，因此，内部控制既有手工控制，也有程序化控制。

依据控制实施部门的不同，可分为电算化部门控制和用户控制。电算化部门控制是指由电算化部门人员或计算机程序实施的控制；用户控制是指会计数据使用部门对计算机数据处理实施的控制。

四、计算机信息系统内部控制的特点

（一）系统开发阶段的控制是其他控制有效地发挥作用的前提

开发计算机信息系统的成本是非常高的，如果设计出来的系统不能满足用户的要求或设计含有错误，那么，即使以后的各项控制措施是严密完善的，也会给单位带来巨大的损失，而且一旦系统投入使用，要修改将是非常困难并要耗费巨额成本的。因此，系统开发阶段必须实行强有力的控制，及时发现和修正错误，并在系统里建立必要的程序控制，在系统设计时，注意留下审计线索或嵌入审计程序，以保证开发出来的系统能满足用户的需求以及今后审计的需要。

（二）控制的重点是电子数据处理部门

在手工信息系统中，每一项经济业务活动都可划分为授权、主办、核准、执行、记录和复核等步骤，并把这些步骤分别交给不同的部门或人员来办理。但在计算机信息系统中，大量的工作都集中到电子数据处理部门，一些职能部门往往只负责原始数据的生成、审核、编码以及分析处理计算机输出的报告。原始数据从输入计算机到记账、报表输出都由计算机自动处理，全部的责任与数据都高度集中于电子数据处理部门。因此，电子数据处理部门应是控制的重点。

（三）部分内部控制自动化和程序化

计算机信息系统的内部控制，除包括许多规章制度外，还包括不少以程序的形式建立在计算机系统中的控制。例如，在计算机会计信息系统中，会计凭证输入后，计算机可自动检查会计科目的编码是否合法、凭证编号是否重复、输入数据是否正确；在处理完一批凭证后，计算机可自动检查借方金额合计是否等于贷方金额合计，如果不等，计算机会给出错误信息，这些都是以程序的形式建立在系统中的控制。

（四）控制的要求更为严格，内容更加扩大

计算机信息系统数据处理比手工信息系统具有更大的风险，要求更为严格，同时控制的内容更加扩大。例如，需要重新划分各种不相容的职务，管理和保护各种机器设备、机房设施以及为数众多的计算机程序和文件，否则，就会造成比手工信息系统更大的危害。

五、风险分析与内部控制设计

(一) 风险

风险是指发生损失的可能性。例如,就一个企业来说,如果钱、账、物由一人管理,就是一种风险。风险是潜在的或可能的损失,一旦受到触发,即具备了一定的条件后,风险就会变成真正的损失。例如,钱、账、物由一人管理,如果这个职员的品德不好,那么当他有机会的时候,就会进行贪污,则风险就变成了真正的损失。

(二) 控制

任何降低风险变成真正损失的可能性的措施,都叫控制。例如,钱、账、物实行三分管,这样就会大大降低风险。在会计工作中,进行复式记账,总账与明细账平行登记,定期进行账证、账账、账实核对,进行试算平衡等,都是为了减少会计工作中错误与舞弊的发生,也就是为了降低会计工作中的风险,这些措施称为会计控制。

(三) 风险分析

评估风险,分析其触发的原因,考虑降低风险的有效控制以及控制可能存在的弱点等,称为风险分析。

由于现代审计在审计工作进行实质性测试阶段之前,都要进行初查测试(即对内部控制进行评审),在初查测试阶段,通过了解一个组织的业务环境、经营情况、所制定的规章制度等,来评价被审单位的内部控制制度的健全性和有效性,也就是进行风险分析。根据分析的结果,来确定实质性审查的范围和重点等。

为了能够定量地描述风险程度,一般用两个影响风险大小的因素加以度量,一个因素是预计每次风险造成的平均损失,另一个因素是预计风险导致实际损失的次数,亦即风险事件发生的频率。通过这两个指标,可以计算出预计未来一定时期内由于风险的存在可能导致的损失。其公式如下:

年度风险损失金额 = 每次风险平均损失额 × 年度风险发生次数

风险分析为内部控制的设计提供了一个数量化的工具。内部控制的设置本身需要增加成本,如额外的人工、设备等,但它同时也可以降低风险,减少未来发生的损失。所以,从成本效益的角度来说,一项控制是否设置,要看由于增设控制而减少的风险是否能够弥补增加控制所需要的支出。如果风险降低程度大于其成本支出,则应增加此控制,否则,不应增加此控制。

例如,某单位的计算机信息系统,由于人力限制,原始凭证未经审核直