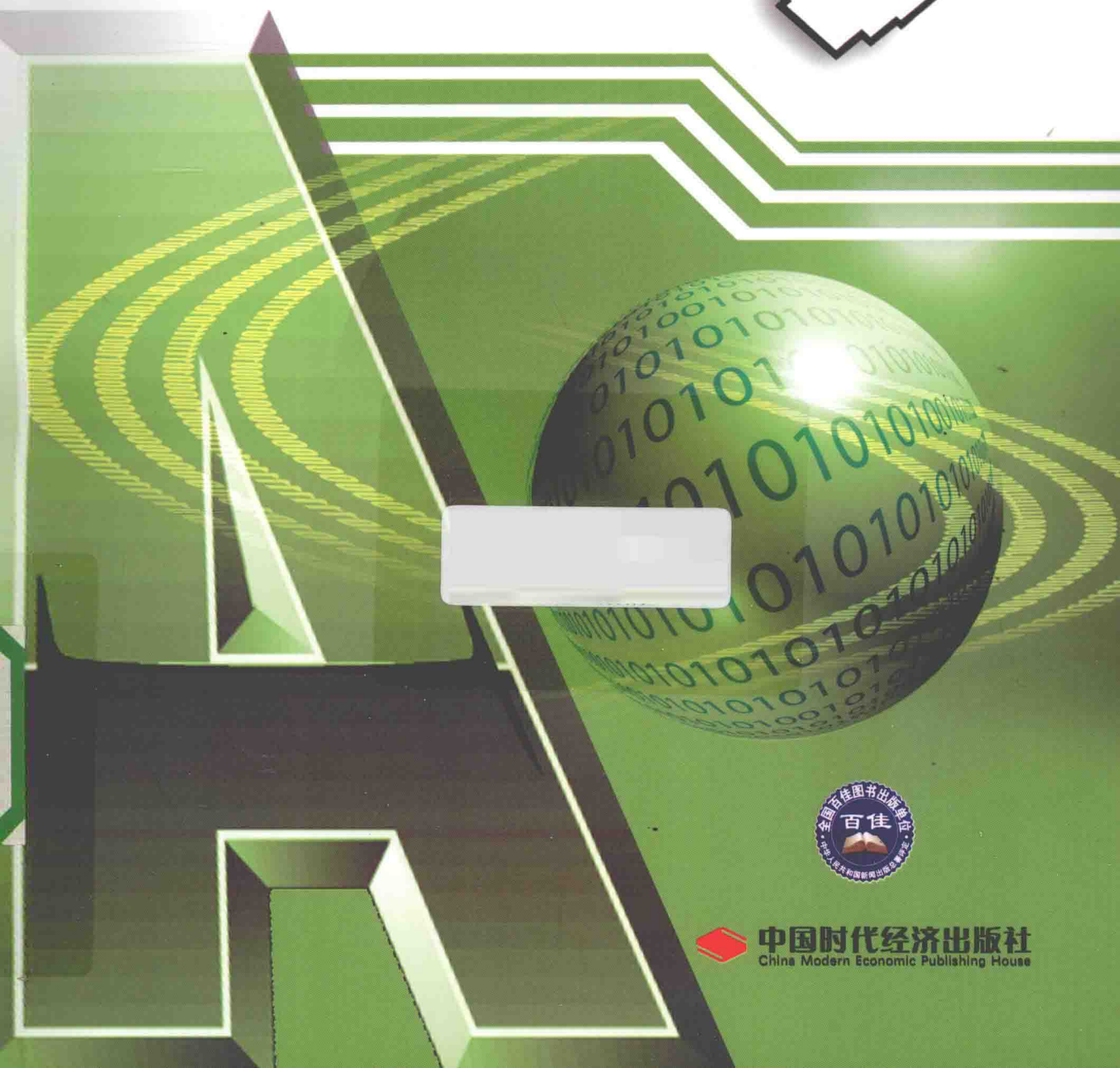
审计署计算机审计中级培训后续课程丛书

信息系统审计

◆本书编写组 编著



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

审计署计算机审计中级培训后续课程丛书

信息系统审计

◆本书编写组 编著

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

图书在版编目（CIP）数据

信息系统审计/《信息系统审计》编写组编著.
—北京：中国时代经济出版社，2014.2
ISBN 978-7-5119-0769-1
Ⅰ.①信… Ⅱ.①信… Ⅲ.①信息系统－审计
Ⅳ.①F239.6
中国版本图书馆 CIP 数据核字（2014）第 018032 号

书　　名：**信息系统审计**
作　　者：《信息系统审计》编写组

出版发行：中国时代经济出版社
社　　址：北京市丰台区玉林里 25 号楼
邮政编码：100069
发行热线：（010）68320825　88361317
传　　真：（010）68320634　68320697
网　　址：www.cmepub.com.cn
电子邮箱：zgsdjj@hotmail.com
经　　销：各地新华书店
印　　刷：北京市昌平百善印刷厂
开　　本：787×1092　1/16
字　　数：226 千字
印　　张：12
版　　次：2014 年 2 月第 1 版
印　　次：2014 年 2 月第 1 次印刷
书　　号：ISBN 978-7-5119-0769-1
定　　价：36.00 元

前　言

伴随政府信息化建设的不断深入推进，目前我国各级政府部门的数字化程度越来越高。层出不穷的各类信息系统成为国家公共政策实施和公共服务的重要载体，系统的数据与信息直接服务于国家的宏观决策，有些系统甚至直接涉及国家秘密信息和高敏感度核心政务。此外，不同行业企事业单位的经济活动越来越多地依赖信息系统开展业务，在提高业务运行效率的同时，信息系统安全风险也日益凸显，信息系统能否满足经济业务活动的需要，能否安全、可靠、有效地运行对于国家信息安全、社会稳定和经济发展具有重要意义。

信息系统审计是根据相关法律法规及标准规范，获得与评估审计证据，对信息系统的安全性、有效性和经济性进行专业判断的过程。信息系统审计是控制信息化风险，提升信息化投资价值的重要手段，审计对象包括计算机硬件、软件、网络、数据和人。信息系统审计的诞生与发展是政府、企事业单位信息化发展到一定程度的必然结果，也是审计现代化转型的必由之路。

近年来，如何控制与监管信息系统建设与运行风险，提高信息化投资绩效，得到了各国审计机关的高度重视。美国审计署早在20世纪80年代就建立了信息系统审计体系，还陆续编制了相当数量的审计指南。英国审计署非常注重IT项目绩效审计。日本政府强调对政府投资的信息系统项目进行全过程审计。世界最高审计组织（INTOSAI）早在2004年就召开工作会议，讨论如何对电子政务系统开展效益审计。我国也不例外，《2006—2020国家信息化发展规划纲要》明确指出要“加强电子政务建设资金投入的审计和监督”。2011年，《审计署“十二五”审计工作发展规划》将“加大对国家信息化建设情况的审计力度，建立电子审计体系，……积极开展对国家信息化政策执行、规划实施和工程建设的审计监督”列为审计工作的六大任务之一。2012年，《审计署关于进一步推进审计信息化建设的指导意见》更是详细提出：“要组织研究和建立对国家电子政务政策规划落实、国家电子政务建设项目的信息共享和业务协同等方面的审计评价指标体系和评价方法，揭示电子政务项目建设中存在的信息不安全、系统不可靠、信息不共享、投资不经济等方面的问题和风险，推动国家电子政务健康发展。”信息系统审计对于信息化风险控制与价值实现的重要作用，已得到各界人士的共识。

对国家审计领域而言，信息系统审计不但是信息化环境下深化我国财政支出审计，更是促进国家信息化建设的健康发展，提升国家治理水平的需要。对于从事审计

实务的广大工作者来说，全面掌握信息系统审计理论与实务相关知识是非常必要的。本书应时而生，在借鉴了美国、日本、英国和澳大利亚等国信息系统审计经验的基础上，结合我国信息系统审计的实践与法规的现状，全面系统地提出了信息系统审计的内容框架及知识体系，书中案例均根据真实案例提炼而成，具有很好的实务操作指导意义。

本书共有7章，第1章概述信息系统审计的概念、内容和组织方式，并归纳总结了国内外信息系统审计相关方面的规范与准则。第2章论述了信息系统审计四个阶段的工作重点，以及安全性审计、经济性审计和生命周期审计等专项审计的内容和技术。第3章重点阐述了总体控制审计的调查信息系统及管理情况、描述分析总体控制状况等五个阶段的关键审计内容与思路。第4章系统讨论了访问控制、配置管理、职责分离和应急计划的审计思路，重点介绍了信息系统安全专项审计的内容与方法。第5章从业务流程控制审计、输入控制审计、处理控制审计和输出控制审计等方面，详细阐述了应用控制审计的内容与程序，还介绍了信息系统绩效审计步骤与评估方法等知识。第6章重点介绍了信息系统审计的常用审计技术方法和工具，包括业务流程描述方法、常用信息系统审计技术方法，以及常用信息系统审计工具等。第7章以具体实务案例的形式，从总体控制审计、一般控制审计和应用控制审计三方面阐述各自的审计内容、思路与方法，并提供一份信息系统审计报告实例供读者参考。

本书由审计署计算机技术中心组织编写，参加编写的工作人员有审计署计算机技术中心曹洪泽、审计署驻济南特派办王大涛、审计署驻南京特派办吴笑凡、青岛市审计局冯占国、南京审计学院余小兵、浙江财经学院唐志豪、国家开发银行稽核评价局刘强。审计署计算机技术中心副主任杨蕴毅在本书的整体结构方面提出了翔实的意见，审订了书稿功能结构、体例设计和样稿，给予了极大的支持，在此表示衷心感谢。

最后，由于审计和信息技术日新月异的发展，信息系统审计理论与实践尚在持续探索之中，书中难免存在不足之处，恳请同行和读者批评指正。

本书编写组

2013年6月

目　录

第1章　信息系统审计概述

信息系统审计是全球关注的话题，是伴随着信息科技的飞速发展而不断发展的新兴审计方式。在我国“信息化带动工业化、工业化促进信息化”建设方针指引下，信息系统日益成为企事业、行政单位信息处理的重要手段，信息技术为信息处理能力和水平的提高提供了强大的支持，同时信息系统的高度复杂性和自动化处理机制也为业务和财务运行带来了风险。因此，被审计单位对信息系统的日益依赖，传统审计载体的变更，促使审计人员更多地关注信息系统，迫使审计人员必须将信息系统审计纳入到审计范围中。

1.1　信息系统审计产生与发展

信息系统审计是顺应信息技术变革而产生的，最初是从国外发展起来的，随着计算机等信息技术手段在审计中的应用，经历了20世纪60年代的萌芽，70年代的发展，80年代的成熟及90年代的普及等多个阶段。

一般认为，信息系统审计的萌芽是从20世纪60年代电子数据处理（EDP）审计开始的。被审计单位的纸质会计资料被电子数据取代，对账务的手工处理变成了计算机操作，审计人员越来越多地关注电子数据的获取、处理及分析，这时信息系统审计的雏形EDP审计应运而生。这一时期的审计模式是作为传统审计方式的扩展发展起来的，较多地集中在国外大型会计师事务所，业务范围是在外部审计中实施信息系统审计。在信息技术应用比较深入的金融机构，还设立了电子数据处理和安全办公室，开始专门评价该部门的电子数据处理和安全，美国海军审计局引进了通用审计软件包。为了对EDP审计进行指导，1969年EDP审计师协会在美国洛杉矶成立。

20世纪70年代，随着计算机应用的普及，利用计算机进行欺诈和舞弊的犯罪事件不断出现。1973年1月，美国“产权基金公司”的保险经营商利用计算机诈骗了数亿美元，负责对其审计的会计师事务所被判赔偿损失，该事件引起了审计界的震惊，美国开始重新重视信息系统应用给审计工作带来的风险，并对EDP审计标准、内部控制评价、信息系统审计方法等问题进行了深入的研究。1978年，美国EDP审计师协会推出了信息系统审计师（CISA）认证考试，成为信息系统审计发展职业化的开端。

进入20世纪80年代，网络和通信技术迅速发展，企业总部与分支机构的信息资源交互与共享使得企业更注重从战略目标出发建立集成信息系统。业务数据与财务数据的大量交互使得审计人员在进行财务审计时必须考虑信息系统的安全、可靠及效率，以保证信息的真实完整。这一时期计算机辅助审计技术得到广泛引用，对信息系统进行直接审查以及运用审计测试技术，审计人员能够更加深入地了解信息系统的开发、程序设计及信息处理的具体过程，开始尝试运用嵌入审计程序的方式开展信息系统审计。

20世纪90年代，信息系统越来越复杂，互联网技术深刻改变着人们的业务处理方式和思维方式，催生了企业的数据大集中及信息系统网络化。集中化的业务处理方式提高了信息共享与资源交互程度的同时，也暴露了业务处理过度依赖信息系统的弱点。因此如何确保网络条件下信息系统的安全、可靠和有效就变得越来越重要。为了更好地实现对信息系统审计的指导，1992年世界最高审计组织（INTOSAI）成立了EDP审计委员会，对成员国的信息系统审计进行指导并相互交流。民间组织方面，1969年美国洛杉矶成立了电子数据处理审计师协会（EDPAA），伴随计算机对被审计单位各个业务环节的影响越来越大，计算机审计也从单纯的关注电子数据处理，延伸到对计算机系统的可靠性、安全性进行了解和评价。1994年，该协会正式更名为信息系统审计与控制协会（ISACA），先后制定了信息系统审计相关的标准、指南和程序，对信息系统审计进行指导，目前ISACA组织已经在全球75个国家和地区建立了185个分支机构。这一阶段在成立职业化国际组织的同时，信息系统审计技术也实现了突飞猛进的发展，标志着信息系统审计在发达国家进入普及阶段。

我国信息系统审计与西方发达国家相比，起步较晚，技术水平相对落后。近年来，审计署与INTOSAI进行了积极的交流与沟通，派出计算机审计骨干赴美学习信息系统审计理念与技术。对国有金融机构、中央企业等信息化程度较高的单位进行了信息系统审计的探索。在审计信息化系统建设项目（“金审工程”）框架下，研究了信息系统审计方法与技术，制定了分行业的数据规划体系，借鉴CISA认证模式培养了一批信息系统审计人才。地方审计机关也积极尝试信息系统审计，在社会保障、财政税收、医疗卫生、交通运输等多个领域做出了有益的探索。

1.2 信息系统审计概念与目标

1.2.1 信息系统审计概念

信息系统审计在不同发展时期内涵有所不同，不同国家各个发展阶段的定义也略有不同，目前尚没有一个统一的定义。信息系统审计领域的权威专家Ron Weber将其定义为，“信息系统审计是一个获取并评价证据，以判断信息系统是否能够保证资产

安全、数据完整以及高效地利用组织的资源，有效地实现组织目标的过程”。日本通产省认为IT审计是“为了信息系统的安全、可靠和有效，由独立于审计对象的IT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检查与评价，向IT审计对象的最高领导层，提出问题与建议的一连串活动”。

综合上述定义可以看出，信息系统审计是由有客观立场的独立审计师实施，包括政府审计机关、内部审计机构中的工作人员，会计师事务所以及独立的信息化鉴证咨询机构等中介组织中的审计师、注册会计师、IT专业人员等；审计的对象是信息系统以及利用组织资源实现的以信息系统为载体的一切活动，包括计算机软硬件组成的信息系统，运行于系统中的业务应用及数据处理活动，保障系统运行的外部环境以及系统生命周期的所有活动等。信息系统的外部审计目标是评价及鉴证，资产是否具备安全性，数据及信息是否具备有效性，利用资源是否具备经济性等，内部审计目标是为领导层提供管理建议、决策支持，帮助其更高效地实现组织目标等。

因此，本书认为信息系统审计是根据相关法律法规及标准规范，在规定的审计范围内，使用业务流程描述、系统测试、数据分析等技术方法，获得与评估审计证据，对信息系统的安全性、有效性和经济性进行专业判断的过程。

1.2.2　信息系统审计目标

在我国国家治理和审计免疫系统理论的指导下，审计机关开展信息系统审计是财政财务收支及相关经济活动的真实合法效益审计的重要组成部分，要融于财政财务收支审计、绩效审计和专项审计调查之中。从我国现实情况出发，信息系统审计的目标应定位于“安全性、有效性、经济性”，以此推动信息系统审计的开展。

信息系统的安全性是指系统的硬件、软件、网络和数据资源是否得到妥善保护，不因自然和人为的因素而遭到破坏、更改或者泄露系统中的信息，审计中要关注信息系统存在的问题或隐患对于国家和被审计单位经济活动安全和信息安全有何重大影响，并对如何防范、消除这些影响提出审计建议。

信息系统的有效性是指系统能否实现既定目标、系统各项业务的处理过程是否符合国家有关法律法规的要求，是否做到真实、完整、准确反映业务处理过程和处理结果。信息系统的有效性与信息系统的业务有关，评价有效性必须对业务有所了解，审计中要关注信息系统功能是否能够支持组织业务目标的实现，系统运行是否可靠，电子数据是否完整可用；系统存在的问题或隐患对于被审计单位主要经济活动和财务指标有何重大影响。

信息系统的经济性一般意义上是指在信息系统建设运行过程中，是否通过较低的资源投入获取合理的预期效果。在经济责任审计中也可以指是否根据经济责任的约定履行了信息系统建设应用责任。信息系统审计中要关注信息系统的建设、开发过程是

否合规；是否有良好的经济效益或社会效益；系统的运行是否实现了建设设计目标；是否给被审计单位的业务运行带来了合理的回报。

1.3 信息系统审计内容体系

我国信息系统审计内容体系，很大程度上借鉴了信息系统控制理论，其内容划分也是从信息系统控制角度表述的，通常可分为总体控制审计、一般控制审计及应用控制审计。在信息系统审计中通过对系统的总体把握、符合性测试、初步评估、关键控制环节分析、实质性审查，逐步形成信息系统审计不同阶段关注的审计内容，审计的重点依不同阶段、不同审计目标而各有侧重。

1.3.1 信息系统审计分类

信息系统审计的对象不仅仅是被审计单位的计算机信息系统，还应包括与信息系统应用及控制有关的各种要素，如系统业务流程、人员管理、数据文件管理和系统运行管理及其执行情况等，都可以作为审计对象。按照不同的标准或维度，可将信息系统审计进行不同的分类。

1. 按照信息系统审计要把握的关键点来划分，信息系统审计分为安全性审计、有效性审计和经济性审计。该审计分类方法是刘家义审计长在审计“免疫系统”理论的框架下提出的，他指出，“在信息化数字化环境下，关注信息系统的可靠性、安全性，是计算机审计中的应有之义，也是我们一直亟待突破的瓶颈。信息系统审计应着重发现控制的风险，并将风险点一一揭露出来，还要注意审计的时效性，问题还没有出现之前就加以揭示，比问题出来后再反映要好”。

2. 按照内部控制在信息系统中的作用与范围不同，信息系统审计分为总体控制审计、一般控制审计和应用控制审计。

（1）总体控制审计。总体控制是指信息系统所处内外环境的控制，通常指管理层及治理层对信息技术治理职能及内部控制重要性的态度、认识和措施等。总体控制审计把信息系统放到被审计单位内外部环境中去分析、评价，关注信息系统的总体状况及主要的风险点，它体现了审计的全面性和系统性，为一般控制和应用控制审计把握重点提供了前提条件。

通常在审计通知书下达后，审计还没有全面开展前，审计人员需要全面了解被审计单位的总体控制情况，结合审计项目的基本要求，针对具体情况采取系列调查和符合性测试分析等多种方法进行信息系统审计的前期工作，并对调查、符合性测试分析结果进行初步的整理，锁定审计领域与审计事项，最终形成指导信息系统审计项目的审计工作方案。

（2）一般控制审计。一般控制是确保信息系统正常运行的制度和工作程序，其主

要目标是保护数据与应用程序的安全，并确保在异常中断情况下计算机信息系统能持续运行。对一般控制的审计中，审计人员应当采用合适的方法、合理的技术手段针对被审计信息系统的安全管理、访问控制、配置管理、职责分离以及应急计划等方面的控制进行检查与测试，以评估信息系统一般控制的效力，也可以为数据审计提供审计线索和依据。

一般控制在被审计单位的组织层面、系统层面实施，其效果是信息系统应用控制效果的决定性因素。如果没有适当的一般控制，应用控制会容易被规避、篡改而导致失效。所以审计工作通常要求对一般控制是否有效进行单独评估，或者在应用控制评估之前实施。

（3）应用控制审计。应用控制是指通过应用系统来实现的业务控制，应用控制审计的目的是评价信息系统的完整性、准确性、有效性、机密性和可用性，进而发现重要财政财务收支以及相关经济活动的问题，揭示系统重大风险。

应用控制可以是人工实施的控制，也可以是由计算机程序实施的自动化控制，应用控制的设计要结合具体业务进行。应用控制审计主要包括业务流程控制审计和数据逻辑控制审计两大类内容。国外信息系统理论中的应用级一般控制被本书归为一般控制审计内容。

3. 按照信息系统发展的生命周期阶段划分，信息系统审计分为系统开发审计、系统验收交付审计和系统运行维护审计。

信息系统遵从客观事物发展规律，存在产生、发展、成熟、消亡或更新的过程，称为信息系统的生命周期，包括系统规划、系统分析、系统设计、系统实施、系统运行五个阶段。各阶段存在相应的风险点及控制活动，从审计角度来说，生命周期审计是对系统的全面审计，要涉及信息系统生命周期的各个阶段，归纳共性特征，主要包括系统开发审计、系统交付验收审计和系统运行维护审计。

1.3.2　信息系统审计内容

信息系统审计的内容是根据审计目标而确定的，信息系统的所有组成部分都是信息系统审计的实体对象，与信息系统业务应用及系统运行相关的内外部环境、与信息系统管理相伴的控制活动均可作为信息系统审计内容。本书借鉴总体控制、一般控制、应用控制的分类体系，以审计分类、审计事项的级次表述如表1－1所示。

1.3.3　信息系统审计组织方式

根据信息系统审计理论和近年来审计机关的探索实践，我国当前的信息系统审计项目组织方式有两种类型：一种是与财政财务收支审计相结合的组织方式，另一种是信息系统专项审计方式。

表1-1 信息系统审计的内容体系

审计分类	审计事项
总体控制审计	外部合规要求
	被审计单位主营业务
	IT治理体系
	IT战略规划
	IT投资政策
	IT运维管理
	信息安全管理制度
	人力资源政策
	内部审计制度
一般控制审计	安全管理
	访问控制
	配置管理
	职责分离
	应急计划
应用控制审计	业务流程控制
	输入控制
	输出控制
	处理控制
	接口控制
	数据库管理
	数据逻辑控制审计

所谓与财政财务收支审计相结合的组织方式，是在财政财务收支审计过程中运用信息系统审计的手段和方法进行审计的组织方式，一般根据财务审计的需要提出。该种组织方式的一种特例情况是：在财政财务收支审计的审计方案中虽未涉及信息系统审计的内容，但是在审计工作中发现与信息系统相关的线索时，调整审计方案，设计审计事项，延伸对信息系统进行审计。在现阶段我国国家审计中，与财政财务收支审计相结合的方式是信息系统审计的主要组织方式。

所谓信息系统专项审计的组织方式，是指审计机关根据对特定行业系统的总体分析，针对那些与国家信息安全或被审计单位经济活动和信息安全密切相关的信息系统，专门组织开展的审计项目或审计调查。有需求的内部审计机构及社会审计组织也可针对特定审计目标开展信息系统专项审计。目前，常见的专项审计组织方式主要有

信息系统安全性审计、信息系统绩效审计以及信息系统生命周期审计等。

不论何种组织方式，信息系统审计组通常应由三部分人员组成，首先是具有审计业务背景与信息技术背景兼备的复合型审计人员，其次是具有信息系统审计专业技能的专业审计人员，最后是具备财政财务收支审计业务能力的审计人员。其中第一部分审计人员是实施信息系统审计的组织者和管理者，通过他们更好地将资源整合起来，组织一支拥有一定专业知识、审计技能和审计经验的综合团队，共同实现审计目标。审计组人员分工应至少具备以下能力：第一层面是复合型审计人员，他们的主要任务是选择信息系统审计领域、确定审计事项、制订工作方案；第二层面是有信息技术背景的专业审计人员，能从控制角度分析确认信息系统的重要控制活动，关键控制点，他们要进行指导和实际完成审查测试控制点、编制审计实施方案；第三层面是财政财务收支审计人员，他们要在上述人员的指导下，协助编写审查测试程序，实施审查测试和补偿性审查以及调查取证工作。

1.4　信息系统审计准则规范

信息系统审计准则规范是开展信息系统审计的依据，国外信息系统审计准则一般由行业内专业的职业团体制定和发布，是职业团体的全体会员共同遵循的行为准则。我国专用的信息系统审计规范相对较少，现有规范体系主要是对一般性的计算机审计方面的规定。审计人员在开展信息系统审计工作时，不能以国外的标准为依据，仅可在工作思路上参考借鉴。

1.4.1　国际信息系统审计准则规范

ISACA 是国际上唯一的信息系统审计专业组织，该组织在职业化道路上一直引领着国际信息系统审计的发展，注重分支机构建设、注重 CISA 职业认证考试的同时，信息系统审计标准的发展和传播更是 ISACA 为该行业做出的杰出贡献。

具体地说，信息系统审计准则是“以管理为核心，法律法规为保障，技术为支撑的信息系统审计框架体系”。信息系统审计准则是一个规范化的管理框架，把审计人员和被审计单位各自的权利、义务和责任等纳入管理框架，解决了各方因为职责不明确而影响信息系统审计质量的问题。目前已颁布信息系统审计准则分为信息系统审计标准、审计指南和作业程序三个层次。

1. 审计标准

审计标准是整个信息系统准则体系的总纲，是制定审计指南和作业程序的基础和依据。审计标准是对信息系统审计和报告的强制性要求，规定了信息系统审计师履行 ISACA 职业道德规定的职业责任的最低限度，以及管理层和其他利益相关人应遵循的与信息系统审计相关的职业要求。截至目前，ISACA 已发布了“审计章程”“审计独

立性”等共16个审计标准，自2005年1月1日起陆续实施。

2. 审计指南

审计指南为审计标准的应用提供了指引，信息系统审计师在审计过程中应考虑如何应用指南以实现审计标准的要求，在应用过程中应灵活运用专业判断并纠正任何偏离准则的行为。审计指南的目标是为如何遵守标准的规定提供更多的信息。截至目前，ISACA已发布了“利用其他审计师的工作”“对审计证据的要求”等共39个审计指南，自1998年6月1日起陆续生效。

3. 作业程序

作业程序提供了信息系统审计师在审计过程中可能遇到的审计程序的示例。作业程序为审计师在审计过程中实现标准的要求提供了相关信息，但并不作为硬性要求。作业程序的目标是为审计师遵循标准要求提供更多的信息。作业程序是对审计标准和指南之外的一种补充，审计人员在审计过程中可以参考作业程序中的相关示例进行审计，在遇到特殊情况的时候可以寻求作业程序的指导。截至目前，ISACA已经发布了“信息系统风险评估”“数字签名”等共11个作业程序，自2002年7月1日起陆续生效。

1.4.2 国内信息系统审计准则规范

我国信息系统审计已得到各方面的高度重视，从国家审计的有关法律法规来看，信息系统审计已经列入审计机关的审计范围。1993年9月1日，审计署发布中华人民共和国审计署令第9号《审计署关于计算机审计的暂行规定》第二条指出，“凡使用计算机管理财政、财务收支及其有关经济活动的被审计单位，审计机关有权采用计算机技术，依法独立对其计算机财务系统进行审计监督”。2001年国务院办公厅颁布的《关于利用计算机信息系统开展审计工作有关问题的通知》（国办发〔2001〕88号）规定，审计机关有权检查被审计单位运用计算机管理财政收支、财务收支的信息系统。在审计机关对被审计单位电子数据真实性产生疑问时，可以对计算机信息系统进行测试。2006年新修订的审计法进一步在法律层次上规定，审计机关有权检查被审计单位运用电子计算机管理财政财务收支电子数据的系统。

2010年最新修订的《中华人民共和国国家审计准则》（简称审计准则）分别就职业胜任能力、审计计划，审计实施、获取审计证据，作出审计结论、出具审计报告等总共12项条款对信息系统审计的目标、内容、方法等做出了规定，表现出鲜明的关注信息系统审计以及信息化环境下开展审计工作的特色。准则首次对信息系统控制情况做出具体定义：“一般控制，即保障信息系统正常运行的稳定性、有效性、安全性等方面的控制；应用控制，即保障信息系统产生的数据的真实性、完整性、可靠性等方面的控制。”

2010年4月审计署颁布了《关于检查信息系统相关审计事项的指导意见》（审计

发〔2010〕48号），对信息系统审计的目标和关注点、审计事项的主要内容、审计事项的分类、开展信息系统审计的组织管理方式以及信息系统审计的方法与工具做出了指导性规定，并明确了需要重点关注的9大类26个审计事项。

2009年起，审计署组织技术力量以研究课题的方式对国家信息系统审计指南体系进行了研究，借鉴了国外的理论研究成果并融入了中国特色的信息系统审计实践，2010年10月课题通过了专家验收评审。2011年审计署印发《审计署办公厅关于印发国家审计指南开发方案的通知》（审办法发〔2011〕192号），明确规定。

2012年，审计署颁布了《信息系统审计指南——计算机审计实务公告第34号》（审计发〔2012〕11号），该指南是中国国家审计指南框架体系下的专业指南之一，对信息系统审计定义、内容、流程和技术方法等做出了详细规定，将推动我国信息系统审计实践逐步走向深入。

本章小结

本章从信息系统审计的产生与发展入手，回顾了国际信息系统审计的发展历程以及我国信息系统审计的现状。提出了信息系统审计的概念，即根据公认的标准及指导规范对业务依赖度较强的信息系统开展证据评价，对信息系统及业务应用的安全性、有效性、经济性等进行专业判断的过程。提出了信息系统审计的三大目标，并分别对三大目标的关注点进行阐述。

本章对信息系统审计分别按审计需要把握的关键点，主流系统控制类型以及信息系统生命周期的阶段进行分类，并借鉴控制理论对信息系统审计的内容体系进行了梳理。从国家审计的角度探讨了信息系统审计的组织方式，即与财政财务收支审计相结合的组织方式和信息系统专项审计方式。

本章从国际、国内两个方面综述了信息系统审计的准则及规范，可以看出国外信息系统审计准则一般由行业内专业的职业团体制定和发布，国内相关准则及规范制定工作被高度重视，但尚未形成体系，正在建设与完善中。

思考题

1. 什么是信息系统审计？
2. 简述信息系统审计的目标及分类方法。
3. 信息系统审计一般包括哪些内容？
4. 简述我国信息系统审计的组织方式。

第2章　信息系统审计基本流程

本章介绍审计机关开展信息系统审计工作时，从审计计划工作开始，经历编制审计工作方案和实施方案，实施符合性测试、实质性审查和补偿性控制审查等审计实施工作，然后出具审计报告，并对重要事项还应进行跟踪完成后续审计的全过程。最后，本章介绍了常见的信息系统专项审计类型，审计人员可视实际情况选择针对信息系统安全性、经济性和生命周期等进行专项审计。

2.1　信息系统审计基本流程概述

信息系统审计的流程是指信息系统审计工作从开始到结束的整个过程，审计人员所采取的系统性工作步骤。信息系统审计一般可以分为审计计划、审计实施、审计报告和后续审计四个阶段，前三个阶段为基本阶段，后续审计为延伸阶段。

审计计划阶段是信息系统审计的准备过程，是信息系统审计活动的开始。计划阶段从论证审计项目开始，通过评估确定是否开展信息系统审计，在总体控制审计的基础上确定审计工作目标和内容，最终编制工作方案，分配审计资源。该阶段的标志性工作是提交信息系统审计工作方案。

审计实施阶段是按照审计工作方案了解和审查测试系统，同时编写、完善和实施审计实施方案的过程。信息系统审计的实施方案既可用于指导审计人员开展审计工作，也可以审计实施过程的记录，它可以有效保存审计资源，提高审计成果的共享程度，保证审计的持续性，从整体上提高审计的质量和效率。该阶段的标志性工作是提交信息系统审计实施方案，取得审计证据及审计工作底稿。

审计报告阶段是审计人员运用职业判断和专业技术知识，评估审计证据，汇总审计工作底稿，总体评价信息系统状况、产生的问题及其影响，做出审计结论，提出审计意见，形成审计报告的过程。该阶段的标志性工作是提交信息系统审计报告。

后续审计阶段本质上是以上三个审计阶段的延伸。后续审计阶段，在报告审计发现和建议后，信息系统审计人员获取和评估相关信息，跟踪检查被审计单位的整改情况，判断审计报告中提出的问题是否已经得到有效解决，并依据被审计单位整改过程中发生的信息系统更新及内部控制变化等情况，分析原有审计建议是否适用和需要修改。