2014

中国计算机审计研究报告

中国审计学会计算机审计分会

信息系统审计研究报告

REPORT SERIES OF IT AUDIT RESEARCHES IN CHINA

中国审计学会计算机审计分会

《信息系统审计研究报告》课题组

中国时代经济出版社

2014

中国计算机审计研究报告

中国审计学会计算机审计分会

信息系统审计研究报告

REPORT SERIES OF IT AUDIT RESEARCHES IN CHINA

中国审计学会计算机审计分会

《信息系统审计研究报告》课题组

中国时代经济出版社

图书在版编目（CIP）数据

信息系统审计研究报告／《信息系统审计研究报告》课题组编．—北京：中国时代经济出版社，2015.11
ISBN 978-7-5119-2480-3

Ⅰ.①信… Ⅱ.①信… Ⅲ.①信息系统—审计—研究报告 Ⅳ.①F239.6

中国版本图书馆 CIP 数据核字（2015）第 250970 号

书　　名：信息系统审计研究报告
作　　者：《信息系统审计研究报告》课题组

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）63508271　63508273
传　　真：（010）63508274　63508284
网　　址：www.cmepub.com.cn
电子邮箱：zgsdjj@hotmail.com
经　　销：各地新华书店
印　　刷：北京嘉恒彩色印刷有限责任公司
开　　本：787×1092　1/16
字　　数：502 千字
印　　张：31.75
版　　次：2015 年 11 月第 1 版
印　　次：2015 年 11 月第 1 次印刷
书　　号：ISBN 978-7-5119-2480-3
定　　价：80.00 元

前　言

2009年，刘家义审计长指出，信息系统审计就是要关注信息系统的安全性、可靠性和经济性。审计署2012年发布的《信息系统审计指南》（计算机审计实务公告第34号）中提出，信息系统审计的主要目标是检查和评价被审计单位信息系统的安全性、可靠性和经济性。2013年以来，中国审计学会计算机审计分会在组织编写上述《信息系统审计指南》的基础上，认真汲取国外信息系统审计成果，结合我国审计实践，进一步研究安全性、可靠性和经济性与信息系统审计框架和结构内容的融合度，形成目前的《信息系统审计研究报告》（以下简称《研究报告》）。

《研究报告》围绕安全性、可靠性和经济性的信息系统审计目标，旨在将三性融入信息系统审计框架和结构内容。为此，我们认真研究了国外信息系统审计框架和结构内容。美国信息系统审计与控制协会（ISACA）于1996年发布的《信息及相关技术的控制目标》（COBIT），规划了按照IT目标（有效性、高效性、机密性、完整性、可用性、符合性、信息可靠性），对IT资源（人、应用系统、技术、设施和数据）的IT过程（规划与组织、获取与实施、交付与支持、监控与评价）进行管控的过程控制审计框架。参照国外信息系统审计框架，结合我国审计实践，《研究报告》提出了按照信息系统控制目标（安全性、可靠性和经济性），对信息系统资源（管理资源、应用资源、网络资源和安全资源）的结构控制（管理控制、应用控制、网络控制和安全控制）进行管控的结构控制审计框架。国外的过程控制审计框架和《研究报告》提出的我国结构控制审计框架，为我国开展信息系统审计提供了更加丰富的信息系统控制知识和实务指导。

《研究报告》提出的我国信息系统结构控制审计框架，旨在将安全性、可靠性和经济性融入信息系统组成要素的结构控制审计：管理控制审计的目标是保障信息系统各类管理的安全、可靠和经济，重点检查其组织管理、规

划管理、建设管理和运行管理的控制有效性；应用控制审计的目标是保障信息系统承载业务和信息资源的安全、可靠和经济，重点检查其应用架构、应用功能、信息资源和共享协同的控制有效性；网络控制审计的目标是保障信息系统网络基础设施的安全、可靠和经济，重点检查其网络结构、网络通信、存储处理和机房系统的控制有效性；安全控制审计的目标是保障信息系统管理和技术的安全、可靠和经济，重点检查其安全架构、安全制度、安全体系和安全功能的控制有效性。管理控制、应用控制、网络控制、安全控制的信息系统结构控制审计框架的规划，既覆盖了信息系统的各个组成要素，也适宜我国信息系统审计的人才培养和审计组织实施。

《研究报告》共为五个部分：第一部分为总论，第二部分为信息系统管理控制审计，第三部分为信息系统应用控制审计，第四部分为信息系统网络控制审计，第五部分为信息系统安全控制审计。第一部分介绍信息系统审计的目标、内容和程序，信息系统审计框架和方法，以及信息系统审计相关法规、标准和信息技术发展。从第二部分到第五部分，每部分各分为四章，每章在介绍信息系统结构控制知识后，提出该类控制的审计控制点和审计方法。

《信息系统审计研究报告》由中国审计学会计算机审计分会组织，课题组成员有：周德铭、曹洪泽、余小兵、刘强、万建国、王彪、李俊、隋学深、刘会齐、王晓敏，周德铭负责框架规划，曹洪泽负责各章审核。《研究报告》得到了王智玉、刘力云、鲍国明、张金城、孙强等专家的悉心指导，在此一并表示感谢！

由于我们水平有限，疏误之处在所难免，敬请信息系统审计同行和各界读者批评指正。

《信息系统审计研究报告》课题组

2014 年 10 月

目　录

第一部分　总论

第二部分 信息系统管理控制审计

第三部分　信息系统应用控制审计

第四部分 信息系统网络控制审计

第五部分　信息系统安全控制审计

第一部分　总论

本部分根据《中华人民共和国国家审计准则》关于审计组织、审计程序、审计质量控制等相关规定，研究了信息系统审计的目标、内容和程序；结合我国审计实践，研究构建了适合我国情况的信息系统审计框架；归集描述了信息系统审计的法规和准则，并概要介绍了信息技术发展情况。

本部分研究内容包括五章：总论，审计目标、内容和程序，审计框架与方法，相关规划和审计规范，信息技术发展。

第一章　概论

本章研究信息系统审计的概念和特点、地位和作用、审计组织方式和适用条件、审计机构和人员素质等方面的内容。

第一节　信息系统审计概述

信息系统审计概述包括信息系统审计的概念、特点以及信息系统审计在国内外发展历程的内容。

一、信息系统审计的概念和特点

1. 信息系统审计的概念

关于信息系统审计的概念，目前业界从不同的角度进行了不同的表述。

观点一：信息系统审计是一个获取并评价证据，以判断计算机系统是否能够保证资产的安全、数据的完整以及有效利用组织的资源并有效果地实现组织目标的过程。

观点二：为了信息系统的安全、可靠与有效，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的检查与评价，向 IT 审计对象的最高领导，提出问题与建议的一连串活动。

我国审计署 2012 年发布的《信息系统审计指南》（计算机审计实务公告第 34 号）将信息系统审计定义为：信息系统审计是指国家审计机关依法对被审计单位信息系统的真实性、合法性、效益性和安全性进行检查监督的活动。

中国内部审计协会 2013 年发布的《第 2203 号内部审计具体准则——信息系统审计》将信息系统审计定义为：信息系统审计是指内部审计机构和内部审计人员对组织的信息系统及其相关的信息技术内部控制和流程所进行的

审查与评价活动。

2014 年，《国务院关于加强审计工作的意见》（国发〔2014〕48 号）要求：创新电子审计技术，提高审计工作能力、质量和效率；推进对各部门、单位计算机信息系统安全性、可靠性和经济性的审计。

综上所述，信息系统审计至少包括四个要素：一是信息系统审计的对象是被审计单位承载业务活动的信息系统及其控制环境。二是信息系统审计的目标是通过审计监督促进信息系统的安全性、可靠性和经济性。三是信息系统审计的内容是检查信息系统的管理控制、应用控制、网络控制和安全控制的有效性。四是信息系统审计的方法主要是利用一般审计方法和技术测评方法，检查信息系统各类控制对于安全性、可靠性和经济性的保障程度。

为此，本报告提出信息系统审计的概念：信息系统审计是指审计组织对被审计单位信息系统的管理控制、应用控制、网络控制和安全控制的安全性、可靠性和经济性进行检查，促进信息系统组织目标实现的监督和评价活动。

2. 信息系统审计的特点

信息系统审计的特点是较之电子数据审计而言，在审计对象、审计目标、审计内容、审计方法等方面的不同特点。

（1）信息系统审计对象特点

在信息化环境下，按照审计对象划分，可以划分为两类：一是被审计单位记载财政收支、财务收支及其相关经济业务活动的电子数据；二是被审计单位管理财政收支、财务收支及其相关经济业务活动的计算机信息系统。

审计对象划分的依据是：2006 年修订的《中华人民共和国审计法》第十六条规定，审计机关对本级各部门（含直属单位）和下级政府预算的执行情况和决算以及其他财政收支情况，进行审计监督。审计机关对前款所列财政收支或者财务收支的真实、合法和效益，依法进行审计监督。第三十一条至三十二条规定，审计机关进行审计时，有权检查被审计单位运用电子计算机储存、处理的财政收支、财务收支的电子数据；有权检查被审计单位运用电子计算机管理财政收支、财务收支电子数据的信息系统。2014 年 6 月 9 日，国务院法制办网上公示的关于《国务院关于修改〈中华人民共和国审计法实施条例〉的决定（征求意见稿）》的说明中新增的第三十八条内容为，审计机关依照审计法第三十二条规定进行检查时，有权检查被审计单位记载财政收支、财务收支及其相关经济业务活动的电子数据的真实性、完整性和可靠

性，以及被审计单位管理财政收支、财务收支及其相关经济业务活动的计算机信息系统的安全性、可靠性和经济性。

由于审计对象的不同，导致审计目标、审计内容、审计方法等一系列审计内涵的不同。在本报告中，从审计对象划分的角度，将审计分为电子数据审计、信息系统审计两大类。

（2）信息系统审计目标特点

电子数据审计的目标是，通过对被审计单位财政财务及其相关经济业务活动的真实性、合法性和效益性的审计监督，维护国家财政经济秩序，提高财政资金使用效益，促进廉政建设，保障国民经济和社会健康发展，发挥国家审计在完善国家治理、维护国家安全和人民根本利益方面的作用。

信息系统审计的目标是，通过对被审计单位信息系统的安全性、可靠性和经济性的审计监督，促进信息系统组织目标的实现，维护国家网络信息安全，保障国民经济和社会信息化的健康发展，发挥国家审计在完善国家治理、维护国家安全和人民根本利益方面的作用。

（3）信息系统审计方法特点

电子数据审计的方法是，主要采用一般审计方法和数据分析方法。一般审计方法包括：审计调查方法、资料审查方法、实地考察方法、专家评审方法、内控评估方法、风险评估方法等。数据分析方法包括：审计查询方法、多维分析方法、数据挖掘方法、模拟仿真预测方法、大数据分析方法等。

信息系统审计的方法是，主要采用一般审计方法和技术测试方法。一般审计方法包括：系统调查方法、资料审查方法、图标审查方法、实地考察方法、专家评审方法、风险评估方法等。技术测试方法包括：安全工具检测、审计工具检测、测评工具检测，以及利用信息系统运行监控的功能和监控信息，进行系统运行监测、系统监控检测等。

二、国外信息系统审计的产生和发展

信息系统审计最初是从国外发展起来的，随着计算机信息技术手段在被审计单位中的应用，信息系统审计经历了萌芽、发展、成熟和普及四个阶段。

1. 萌芽阶段

20 世纪 60 年代，随着计算机信息技术手段的应用，越来越多的被审计单位的会计信息处理实现了电算化。纸质的会计资料变成了电子数据，手工

处理也被电子数据处理（Electronic Data Processing，EDP）所代替。为了对被审计单位做出客观的评价，审计人员越来越多地关注电子数据的取得、分析和计算等过程，信息系统审计的雏形——EDP 审计随之产生。这一时期，许多国外大型的会计师事务所在外部审计中开始实施信息系统审计，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，开始专门评价本部门的电子数据处理和安全。在信息系统审计理论上，一些专家学者也进行了积极探索。美国学者 F. 坎夫曼 1961 年出版了第一本有关信息系统审计的著作《电子数据处理和审计》。IBM 公司也出版了 *Audit Encounters Electronic Data Processing* 及 *In-line Electronic Processing and Audit Trail* 等文献，制定了电子数据环境下的内部审计规则和组成方法，介绍了许多新的概念、术语和审计技术。1968 年美国注册会计师协会（AICPA）出版了《会计审计与计算机》一书，阐述了在电子数据处理环境下如何开展信息系统审计和传统的外部审计。为了对 EDP 审计进行指导，EDP 审计师协会于 1969 年在洛杉矶成立。在这个阶段，信息系统审计虽然已经萌芽，但审计人员对信息系统审计的认识还很不够，信息系统审计实务开展尚未普及。

2. 发展阶段

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也开始出现。1973 年 1 月，美国“产权基金公司”的保险经营商利用计算机进行欺诈，诈骗金额高达数亿美元，负责该公司审计的事务所也被判赔偿损失，这件事情引起了美国审计界的震惊，使得人们开始重视信息系统审计。由于舞弊和欺诈事件的发生，对 EDP 审计的需求迅速增加，计算机辅助审计技术在实践中也得到初步运用。在信息系统审计理论方面，1974 年 AICPA 发表了《内部控制的调查与评价对电子数据处理的影响》，成为对电子数据处理系统实施审计的标准。1977 年美国内部审计师协会在对美国、加拿大、欧洲、日本等地企业调查研究的基础上，发表了著名的《系统可审性及规则的研究》，即 SAC 报告。SAC 报告提出的很多计算机辅助审计技术，是利用计算机直接对信息系统进行审核检查的开创性探索。1975 年日本情报处理开发协会成立了 ISA 委员会，开始了信息系统审计的研究。通过组织几批访美的考察团，了解美国实施信息系统审计的情况，并发表了研究报告。日本注册会计师协会 1976 年发表了《使用电子计算机的会计组织的内部规则质问书（修订案）》《EDP 审计标准及审计过程试案》《EDP 审计方法》等，

并明确了这些文件为 EDP 审计师必须遵循的标准。1978 年美国信息系统审计与控制协会（ISACA 组织）推出了信息系统审计师（CISA）考试与认证，成为信息系统审计职业化发展的开端。

3. 成熟阶段

20 世纪 80 年代，计算机和网络通信技术的结合，进一步促进了信息系统审计的发展，计算机辅助审计技术得到广泛应用。越来越多的审计人员开始在审计中应用信息系统审计测试技术，对信息系统进行直接审查。运用这些先进的审计技术，审计人员能够更加深入地了解被审计单位信息系统的开发、程序设计和信息处理的具体过程和内容，从而能够更为有效地开展信息系统审计工作。有些审计人员甚至可以利用嵌入审计程序的方法对信息系统进行审计。在信息系统审计理论方面，美国 EDP 审计师协会 1984 年发布了《EDP 控制的目标》，提出了信息系统的控制标准。1987 年发布了《信息系统审计的基本准则》（*General Standards for Information Systems Auditing*），提出了信息系统审计的基本标准。1982 年日本通产省在机械信息产业局中设立了“计算机安全研究会”，研究信息化健全发展的必要法规。1983 年发表了通产省紧急课题“计算机安全的研究”成果《有关计算机的安全对策》。1984 年日本政府委托情报化对策委员会 ISA 协会对美国的 IT 审计标准进行了研究，第二年通产省发表了《IT 审计标准》，指出仅仅只有系统的内部审计是不够的，要引入第三方（信息系统审计师）对信息系统的安全性、可靠性进行全面检查，并在日本的软件水平考试中增添“IT 审计师”的内容。信息系统审计测试技术的发展以及信息系统审计标准研究的提出标志着信息系统审计进入成熟阶段。

4. 普及阶段

20 世纪 90 年代，信息系统日益复杂化、大型化、网络化，并且在互联网技术的支持下，深刻改变着人们业务处理的方式和思维方式，其广度和深度是任何产业革命所无法比拟的。信息系统和互联网使得信息资源作用充分发挥的同时，也产生了很多不安全的因素。因特网作为大型业务系统信息处理的平台，同时也成为计算机犯罪的场所。信息系统集中化的业务处理方式提高了信息共享程度，也暴露了信息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。为了对信息系统审计进行指导，1994 年 EDP 审计师协会正式更名为信息系统审计