第一章　信息系统审计基础法规知识

第一节　信息系统审计概论

1. 信息系统审计概念

■ 2012 年 2 月，审计署《信息系统审计指南》（审计发〔2012〕11 号）：

第二条　本指南所称信息系统，是指被审计单位利用现代信息技术实现财政收支、财务收支及其相关经济业务活动的信息处理的系统。

本指南所称信息系统审计，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。

■ 2014 年 1 月，中国内部审计协会《第 2203 号内部审计具体准则——信息系统审计》：

第二条　本准则所称信息系统审计，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。

2. 信息系统审计目标

■ 2014 年 1 月，中国内部审计协会《第 2203 号内部审计具体准则——信息系统审计》：

第四条　信息系统审计的目的是通过实施信息系统审计工作，对组织是否实现信息技术管理目标进行审查和评价，并基于评价意见提出管理建议，协助组织信息技术管理人员有效地履行职责。组织的信息技术管理目标主要包括：

（一）保证组织的信息技术战略充分反映组织的战略目标；

（二）提高组织所依赖的信息系统的可靠性、稳定性、安全性及数据处理的完整性和准确性；

（三）提高信息系统运行的效果与效率，合理保证信息系统的运行符合法律法规以及相关监管要求。

■ 2012 年 2 月，审计署《信息系统审计指南》（审计发〔2012〕11 号）：

第六条　信息系统审计的主要目标是通过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，揭示信息系统存在的问题，提出完善信息系统控制的审计意见和建议，促进被审计单位信息系统实现组织目标；同时，通过检查和评价信息系统产生数据的真实性、完整性和正确性，防范和控制审计风险。

■ 2014 年 10 月，《国务院关于加强审计工作的意见》（国发〔2014〕48 号）：

（十九）加快推进审计信息化。推进有关部门、金融机构和国有企事业单位等与审计机关实现信息共享，加大数据集中力度，构建国家审计数据系统。探索在审计实践中运用大数据技术的途径，加大数据综合利用力度，提高运用信息化技术查核问题、评价判断、宏观分析的能力。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。

3. 信息系统审计权限

■ 2001 年 11 月 16 日，《国务院办公厅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）：

一、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（以下简称计算机信息系统）。被审计单位应当按照审计机关的要求，提供与财政收支、财务收支有关的电子数据和必要的计算机技术文档等资料。审计机关在对计算机信息系统实施审计时，被审计单位应当配合审计机关的工作，并提供必要的工作条件。

被审计单位拒绝、拖延提供与审计事项有关的电子数据资料，或者拒绝、阻碍检查的，由审计机关按照《中华人民共和国审计法实施条例》第四十九条的规定处理。

■ 2006 年 2 月 28 日，第十届全国人民代表大会常务委员会第二十次会议修正《中华人民共和国审计法》：

第三十一条　审计机关有权要求被审计单位按照审计机关的规定提供预算或者财务收支计划、预算执行情况、决算、财务会计报告，运用电子计算机储存、处理的财政收支、财务收支电子数据和必要的电子计算机技术文档，在金融机构开立账户的情况，社会审计机构出具的审计报告，以及其他与财政收支或者财务收支有关的资料，被审计单位不得拒绝、拖延、谎报。

被审计单位负责人对本单位提供的财务会计资料的真实性和完整性负责。

第三十二条　审计机关进行审计时，有权检查被审计单位的会计凭证、会计账簿、财务会计报告和运用电子计算机管理财政收支、财务收支电子数据的系统，以及其他与财政收支、财务收支有关的资料和资产，被审计单位不得拒绝。

■ 2010 年 2 月 11 日，国务院颁布《中华人民共和国审计法实施条例》（中华人民共和国国务院令 2010 年第 571 号）：

第二十八条　审计机关依法进行审计监督时，被审计单位应当依照审计法第三十一条规定，向审计机关提供与财政收支、财务收支有关的资料。被审计单位负责人应当对本单位提供资料的真实性和完整性作出书面承诺。

■ 2014 年 10 月，《国务院关于加强审计工作的意见》（国发〔2014〕48 号）：

（十一）依法接受审计监督。凡是涉及管理、分配、使用公共资金、国有资产、国有资源的部门、单位和个人，都要自觉接受审计、配合审计，不得设置障碍。有关部门和单位要依法、及时、全面提供审计所需的财务会计、业务和管理等资料，不得制定限制向审计机关提供资料和开放计算机信息系统查询权限的规定，已经制定的应予修订或废止。对获取的资料，审计机关要严格保密。

（十二）提供完整准确真实的电子数据。有关部门、金融机构和国有企事业单位应根据审计工作需要，依法向审计机关提供与本单位、本系统履行职责相关的电子数据信息和必要的技术文档；在确保数据信息安全的前提下，协助审计机关开展联网审计。在现场审计阶段，被审计单位要为审计机关进行电子数据分析提供必要的工作环境。

（二十二）维护审计的独立性。地方各级政府要保障审计机关依法审计、依法查处问题、依法向社会公告审计结果，不受其他行政机关、社会团体和个人的干涉，定期组织开展对审计法律法规执行情况的监督检查。对拒不接受审计监督，阻挠、干扰和不配合审计工作，或威胁、恐吓、报复审计人员

的，要依法依纪查处。

4. 信息系统审计职业要求

2010 年 9 月，《中华人民共和国国家审计准则》（中华人民共和国审计署令 2010 年第 8 号）：

第十二条　审计机关和审计人员执行审计业务，应当具备本准则规定的资格条件和职业要求。

第十三条　审计机关执行审计业务，应当具备下列资格条件：

（一）符合法定的审计职责和权限；

（二）有职业胜任能力的审计人员；

（三）建立适当的审计质量控制制度；

（四）必需的经费和其他工作条件。

第十四条　审计人员执行审计业务，应当具备下列职业要求：

（一）遵守法律法规和本准则；

（二）恪守审计职业道德；

（三）保持应有的审计独立性；

（四）具备必需的职业胜任能力；

（五）其他职业要求。

第十五条　审计人员应当恪守严格依法、正直坦诚、客观公正、勤勉尽责、保守秘密的基本审计职业道德。

严格依法就是审计人员应当严格依照法定的审计职责、权限和程序进行审计监督，规范审计行为。

正直坦诚就是审计人员应当坚持原则，不屈从于外部压力；不歪曲事实，不隐瞒审计发现的问题；廉洁自律，不利用职权谋取私利；维护国家利益和公共利益。

客观公正就是审计人员应当保持客观公正的立场和态度，以适当、充分的审计证据支持审计结论，实事求是地作出审计评价和处理审计发现的问题。

勤勉尽责就是审计人员应当爱岗敬业，勤勉高效，严谨细致，认真履行审计职责，保证审计工作质量。

保守秘密就是审计人员应当保守其在执行审计业务中知悉的国家秘密、商业秘密；对于执行审计业务取得的资料、形成的审计记录和掌握的相关情况，未经批准不得对外提供和披露，不得用于与审计工作无关的目的。

第十六条　审计人员执行审计业务时，应当保持应有的审计独立性，遇有下列可能损害审计独立性情形的，应当向审计机关报告：

（一）与被审计单位负责人或者有关主管人员有夫妻关系、直系血亲关系、三代以内旁系血亲以及近姻亲关系；

（二）与被审计单位或者审计事项有直接经济利益关系；

（三）对曾经管理或者直接办理过的相关业务进行审计；

（四）可能损害审计独立性的其他情形。

第十七条　审计人员不得参加影响审计独立性的活动，不得参与被审计单位的管理活动。

第十八条　审计机关组成审计组时，应当了解审计组成员可能损害审计独立性的情形，并根据具体情况采取下列措施，避免损害审计独立性：

（一）依法要求相关审计人员回避；

（二）对相关审计人员执行具体审计业务的范围作出限制；

（三）对相关审计人员的工作追加必要的复核程序；

（四）其他措施。

第十九条　审计机关应当建立审计人员交流等制度，避免审计人员因执行审计业务长期与同一被审计单位接触可能对审计独立性造成的损害。

第二十条　审计机关可以聘请外部人员参加审计业务或者提供技术支持、专业咨询、专业鉴定。

审计机关聘请的外部人员应当具备本准则第十四条规定的职业要求。

第二十一条　有下列情形之一的外部人员，审计机关不得聘请：

（一）被刑事处罚的；

（二）被劳动教养的；

（三）被行政拘留的；

（四）审计独立性可能受到损害的；

（五）法律规定不得从事公务的其他情形。

第二十二条　审计人员应当具备与其从事审计业务相适应的专业知识、职业能力和工作经验。

审计机关应当建立和实施审计人员录用、继续教育、培训、业绩评价考核和奖惩激励制度，确保审计人员具有与其从事业务相适应的职业胜任能力。

第二十三条　审计机关应当合理配备审计人员，组成审计组，确保其在整体上具备与审计项目相适应的职业胜任能力。

被审计单位的信息技术对实现审计目标有重大影响的，审计组的整体胜任能力应当包括信息技术方面的胜任能力。

第二十四条　审计人员执行审计业务时，应当合理运用职业判断，保持职业谨慎，对被审计单位可能存在的重要问题保持警觉，并审慎评价所获取审计证据的适当性和充分性，得出恰当的审计结论。

第二十五条　审计人员执行审计业务时，应当从下列方面保持与被审计单位的工作关系：

（一）与被审计单位沟通并听取其意见；

（二）客观公正地作出审计结论，尊重并维护被审计单位的合法权益；

（三）严格执行审计纪律；

（四）坚持文明审计，保持良好的职业形象。

第二节　信息系统审计框架与方式

5. 信息系统结构控制审计框架

中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第三章　审计框架与方法

第一节　信息系统控制审计框架

二、我国信息系统结构控制审计框架

我国信息系统审计十多年实践中，积极探索了信息系统结构控制的审计框架。2012 年，我国审计署发布的《信息系统审计指南》，把信息系统建设项目管理从一般控制中分离出来，形成了项目管理、应用控制、一般控制三要素结构的信息系统控制审计方法。2013 年，中国内部审计协会发布的《第 2203 号内部审计具体准则——信息系统审计》，把信息系统组织层面从一般控制中分离出来，构建了组织层面、一般性控制层面、业务流程即应用层面三要素结构的信息技术风险评估方法。同时，在我国的信息系统审计实践中，多数是在财政财务收支审计中结合开展信息系统审计。这种数据式系统基础审计方式的特点是，重点关注系统内部控制缺失可能导致的数据风险，并以

应用系统中的应用软件和数据库内部控制为切入点，如果发现存在数据风险再根据需要关联分析网络系统中的网络通信和存储处理控制、安全系统中的应用安全和数据安全控制等，在此基础上向审计组提出数据风险的报告，避免财政财务收支审计假账真查。这种审计方式是典型的信息系统结构控制审计。

所谓信息系统结构控制审计框架，是指按照信息系统控制目标（信息系统的安全性、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）进行管控的三维框架。

信息系统结构控制审计框架中呈现的管理控制、应用控制、网络控制和安全控制的四类结构控制域，是由信息系统的内在属性决定的：信息系统的规划、建设和运行，属于管理控制的范畴；信息系统承载业务的业务流程、业务信息等，属于应用控制的范畴；保障多组织间业务流程和业务信息流转的实现路径，属于网络控制的范畴；保障业务信息和系统运行的安全，属于安全控制的范畴。信息系统审计关注四类控制的符合性和有效性，形成了四类结构控制的审计框架。

6. 信息系统管理控制审计框架

中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第三章　审计框架与方法

第一节　信息系统控制审计框架

三、信息系统管理控制审计框架

信息系统管理控制审计框架由管理控制目标、管理控制环节、管理控制资源三要素组成。

管理控制目标是：通过加强管理控制的各个控制环节和控制点的控制策略和措施，保障信息系统建设和运行的可靠性、安全性、经济性，促进组织目标的实现。

管理控制需要从组织领导管理和建设项目管理两个层面加强，包括组织管理、规划立项、建设管理和运行管理 4 个具体控制。

组织管理控制。一是组织机构管理控制。包括信息化领导机构、实施机

构、监督机构、专家咨询、IT服务资源等控制点。二是制度管理控制。包括信息系统发展规划、管理制度、标准规范、设计规范、操作规程等控制点。三是队伍建设管理控制。包括信息化队伍培养规划、综合素质培养、队伍建设激励机制等控制点。

规划管理控制。一是信息化发展规划等控制点。包括信息化建设思路、原则，信息化发展规划的目标、任务和保障措施等控制点。二是需求分析控制。包括组织法定职责分析、组织履职面临的问题或需要改进问题的分析、问题产生的症结及其信息化能力不足的分析、组织解决问题的信息系统目标和考核指标分析、信息化业务需求和业务模型及要素分析、业务要素对信息系统功能和性能的影响等控制点。三是业务模型类型控制。包括政务部门的事务处理类、为民服务类、监测监管类、社会管理类、应急处置类、行政执法类等；企业的销售业务类、供应业务类、生产业务类、财务管理类、人力资源类、经营组织类、企业决策类等对信息系统的影响控制点。四是业务模型要素控制。包括业务逻辑、业务流程、业务信息、业务处理、业务性能、业务部署等对信息系统的影响控制点。五是项目立项管理控制。包括建设项目立项程序管理、立项报告编制管理、立项评估审核和后评价管理等立项管理控制。

建设管理控制。即从信息系统建设项目立项审批起至项目验收的全过程管理控制。一是项目招标管理控制。包括招标投标管理控制、政府采购管理控制等控制点。二是项目实施管理控制。包括详细设计项目管理、监理项目管理、集成项目管理、施工项目管理、应用研发项目管理、系统试运行管理等控制点。三是项目投资管理控制。包括建设项目预算执行管理、项目投资概算调整管理、项目采购合同管理、信息资产管理、项目竣工决算编制与审核管理等控制点。四是项目验收管理控制。包括建设项目单项验收管理、初步验收管理、竣工验收管理等控制点。

运行管理控制。一是运行维护管理控制。包括运维机构职责履行管理、运维制度和运行操作规程管理、运维人员管理等控制点。二是业务应用服务控制。包括远程应用服务、现场应用服务、应用培训服务、应用知识服务等控制点。三是系统运行服务体控制。包括系统运行监控管理、系统运维服务管理、系统运维服务方式管理等控制点。

7. 信息系统应用控制审计框架

中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第三章　审计框架与方法

第一节　信息系统控制审计框架

四、信息系统应用控制审计框架

信息系统应用控制审计框架由应用控制目标、应用控制环节、应用控制资源三要素组成。

应用控制目标是：通过加强应用控制的各个控制环节和控制点的控制策略和措施，保障应用系统和承载业务信息运行的安全性、可靠性和经济性，保障信息资源的完整有效和共享协同。

根据应用控制目标要求，依据信息系统承载业务需求，应用控制包括应用架构控制、应用功能控制、信息资源控制和共享协同控制 4 个具体控制。

应用架构控制。一是满足业务类型的应用架构控制。包括政务信息化的事务处理类、为民服务类、监测监管类、社会管理类、应急处置类、行政执法类等；企业信息化的销售业务类、供应业务类、生产业务类、财务管理类、人力资源类、经营组织类、企业决策类等控制点。二是应用系统的技术架构。包括应用展示层、应用功能层、应用支撑层、信息资源层等控制点。三是应用系统的集约化架构。包括同一功能组件在相关软件功能中的复用集约化、同一软件在相关业务应用中的复用集约化、应用功能在不同建设时期的持续利用和发展、应用系统在行业中的部署复用等控制点。

应用功能控制。一是数据输入控制。包括人工录入控制、数据采集控制、系统交换控制等控制点。二是数据处理控制。包括数据验证控制、数据清洗控制、数据整理控制、数据转换控制、计量和计价处理功能控制、数据计算控制、数据汇总控制、数据分析控制等控制点。三是数据输出控制。包括数据屏幕显示控制、数据打印和复印控制、数据刻录控制、数据交换控制、数据共享控制、数据备份控制等控制点。四是应用系统产品功能控制。包括定制软件、商用软件、专用软件、操作系统、数据库、中间件、功能组件、开源系统软件、国外软件等适用性功能等控制点。

信息资源控制。一是数据规划控制。包括信息资源目录体系、元数据、

主数据、数据元素、财务数据、业务数据、基础数据、分析数据、内部数据、外部数据等控制点。二是数据库设计控制。包括数据库需求设计、概念设计、逻辑设计、物理设计、数据集市、主题数据、用户视图和数据仓库等数据库设计控制点。三是数据库管理控制。包括数据集中式管理、分布式管理、虚拟化管理、数据物理存储管理、数据内存处理管理等控制点。四是数据备份管理。包括数据在线备份、近线备份、同城备份、异地备份、数据恢复等控制点。五是数据分析模型控制。包括查询分析、多维分析、挖掘分析、模拟仿真分析等模型控制点。六是数据访问控制。包括应用访问、数据库直接访问、远程访问、文件检索访问等控制点。

共享协同控制。一是信息共享控制。包括共享平台、共享交口、共享方式、共享目录、共享资源、共享信息元数据、共享信息元素、共享信息格式、单位内部共享、行业内部共享、向社会发布共享等控制点。二是信息交换控制。包括交换平台、交换接口、交换方式、交换目录、交换资源、交换信息元数据、交换信息元素、交换信息格式、单位内部交换、行业内部交换、行业间交换等控制点。三是业务协同控制。包括应用系统内部协同、应用系统间协同、单位内部协同、行业内部协同、行业间协同等控制点。

8. 信息系统网络控制审计框架

中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第三章　审计框架与方法

第一节　信息系统控制审计框架

五、信息系统网络控制审计框架

信息系统网络控制审计框架由网络控制目标、网络控制环节、网络控制资源三要素组成。

网络控制目标是：通过加强网络控制的各个控制环节和控制点的控制策略和措施，保障网络结构、网络通信、存储处理和机房系统的安全性、可靠性和经济性。

根据网络控制目标要求，依据信息系统承载业务需求，网络控制包括网络结构控制、网络通信控制、存储处理控制和机房系统控制 4 个具体控制。

网络结构控制。一是业务部署方式的网络结构控制。包括局域网、城域

网、广域网等控制点。二是局域网分域网络结构控制。包括接入域、交换域、应用域、数据域、用户域、安全域等控制点。三是业务信息不同密级的网络结构控制。包括互联网域、非涉密网络域、高安全防护网络域等控制点。四是网络布线控制。包括电缆网线、光纤网线、无线网、水平和垂直网桥架、面板模块等控制点。五是网络产品功能控制。包括路由器、交换机、网关、网络流量控制、IP 规划、域名规划、网络协议等控制点。

网络通信控制。一是局域网通信控制。包括局域网的接入域、交换域、应用域、数据域、用户域、安全域间等网络通信等控制点。二是广域网通信控制。包括中央城域网、中央至省级主干网、省级城域网、省至市级主干网、市级城域网、市至县级主干网、县级城域网等控制点。三是不同密级网络间通信控制。包括互联网与非涉密网络间、非涉密网络与互联网逻辑隔离状况下与高安全防护网络的通信、非涉密网络与互联网物理隔离状况下与高安全防护网络的通信、互联网与高安全防护网络间的通信等控制点。四是移动网与固定网间的通信控制。包括利用专用网、互联网、无线网间通信等控制点。五是网络带宽控制。包括局域网网络带宽、局域网与城域和广域网间的网络带宽、满足传输高峰值的网络带宽等控制点。

存储处理控制。一是存储方式控制。包括集中存储、分布存储、虚拟化存储、云存储等控制点。二是存储量控制。包括数据存储需求量、设备存储量、实际存储量等控制点。三是存储处理及性能控制。包括大数据处理、并行处理、交易处理、计算处理、会话处理、请求响应等控制点。四是存储处理产品功能控制。包括服务器、存储设备、磁带库、计算机终端、移动终端（平板电脑、手机）、显示屏、打印机、刻录机、移动介质等产品及功能等控制点。

机房系统控制。一是机房功能布局控制。包括网络接入域、数据存储域、应用处理域、互联网域、非涉密网域、高安全防护网域、系统监控域、弱电井域等控制点。二是机房结构控制。包括机房楼板承重、机房防雷接地等控制点。三是机房保障系统控制。包括供电、消防、新风空调、监视监控、温湿度、烟感温感和报警等控制点。四是机房设备产品功能控制。包括网络机柜、服务器机柜、不间断电源（UPS）、空调设备、消防设备、监视设备等控制点。

9. 信息系统安全控制审计框架

中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第三章　审计框架与方法

第一节　信息系统控制审计框架

六、信息系统安全控制审计框架

信息系统安全控制审计框架由安全控制目标、安全控制环节、安全控制资源三要素组成。

安全控制目标是：通过加强安全控制的各个控制环节和控制点的控制策略和措施，保障系统业务信息安全，保障系统运行服务安全。

根据安全控制目标要求，依据信息系统承载业务的信息安全需求，安全控制包括安全架构控制、安全制度控制、安全体系控制和安全功能控制 4 个具体控制。

安全架构控制。一是安全策略控制。包括以安全促发展和以发展求安全、安全制度标准管理策略、业务特征安全策略等控制点。二是安全总体架构控制。包括一个中心、两大体系、三重防护、五个重点等控制点。三是应用安全架构控制。包括数据输入、处理、输出、信息共享、信息交换、不相容职责分离、身份认证和权限控制等控制点。四是网络安全架构控制。包括互联网与非涉密网络间的双向交换隔离控制、非涉密网络与互联网逻辑隔离条件下同高安全防护网络通信的单向导入隔离控制、非涉密网络与互联网物理隔离条件下与高安全防护网络通信的双向交换隔离控制、互联网与高安全防护网络间加密通信控制、跨不可控区域高安全防护网络之间的网络加密传输控制、网络攻击防御、可信计算环境、数据加密存储、网络布线防辐射、计算机屏幕防辐射、违规外联防御、屏蔽机房等控制点。

安全制度控制。一是信息安全等级保护制度。包括信息安全等级保护目标、等级保护实施程序、等级保护定级与报备、等级保护方案与建设实施、等级保护测评与批准、等级保护检查与问题整改等控制点。二是信息安全风险评估。包括安全风险评估制度、风险评估内容、建设单位风险评估实施、专业机构风险测评、风险评估项目竣工验收等控制点。三是网络信息安全应急预案制度。包括应急预案的组织和程序、安全事件的分类与分级、应急响

应的分类与分级、应急响应评估等控制点。

安全体系控制。一是信息安全技术体系控制。包括物理安全的物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护；网络安全的结构安全、访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范、网络设备防护；主机安全的身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范、恶意代码防范、资源控制；应用安全的身份鉴别、访问控制、安全审计、剩余信息保护、通信完整性、通信保密性、抗抵赖、软件容错、资源控制；数据安全的数据完整性、数据保密性、备份和恢复等控制点。二是信息安全管理体系控制。包括安全管理制度的管理制度、制定和发布、评审和修订；安全管理机构的岗位设置、人员配备、授权和审批、沟通和合作、审核和检查；人员安全管理的人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理；安全建设管理的系统定级、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、系统备案、等级测评、安全服务商选择；安全运维管理的环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、网络安全管理、系统安全管理、恶意代码防范管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理等控制点。

安全功能控制。一是加密产品与功能控制。包括核密加密机、普密加密机，MPLS VPN、IPSEC VPN、SSL VPN、认证机构（CA）、公钥基础设施（PKI）、特权管理基础设施（PMI）等控制点。二是高安全防护产品与功能控制。包括信息安全单项导入隔离设备、信息安全双向交换隔离设备等控制点。三是信息安全产品与功能控制。包括入侵检测、漏洞扫描、黑白电源、光电转换器、屏蔽机柜等控制点。

10. 信息系统审计方式

■ 2012 年 2 月，审计署《信息系统审计指南》（审计发〔2012〕11 号）：

第八条　审计人员可以根据审计实施方案要求，选择应用控制、一般控制和项目管理中的相关内容组织实施。

结合经济业务活动审计项目开展的信息系统审计，可以按照审计实施方案要求，重点选择信息系统中容易产生数据风险的内容（见附录），也可以

根据需要选择其他内容组织实施。

独立组织开展的信息系统审计项目，可以按照审计实施方案要求，选择本指南所述的全部或者部分内容组织实施。

■ 中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第一章　概论

第三节　审计组织方式及其适用条件

在信息化环境下，对财政财务收支及其经济活动的审计有两类目标：一是经济活动的真实性、合法性和效益性，这是保障经济活动健康运行的本质性目标。二是信息系统的安全性、可靠性和经济性，这是支撑经济活动健康运行的保障性目标。

在通常情况下，组织对经济活动的完整性审计，应当包括上述两个目标，即在检查经济活动的真实性、合法性和效益性的同时，需要检查经济活动所依赖的信息系统的安全性、可靠性和经济性，防止信息系统内控缺失带来的数据风险，降低审计风险。此时的信息系统审计是结合经济活动审计开展的，我们称之为结合式信息系统审计方式。

在审计计划安排或审计受托情况下，需要对信息系统的立项、建设、运行的安全性、可靠性和经济性独立组织审计。此时的信息系统审计称之为独立式信息系统审计方式。

由于结合式和独立式信息系统审计方式在上述适用条件的不同，在审计计划和审计方案、审计重点、审计程序、审计报告等方面也有所不同。

■ 庄明来、吴沁红、李俊编写的《信息系统审计内容与方法》，中国时代经济出版社 2008 年出版：

根据与财务审计的关系，可以把信息系统审计分为与财务审计相结合的信息系统审计和专门进行的信息系统审计。相应的，信息系统审计的组织方式也可以分为与财务审计相结合的组织方式和专门进行的组织方式。

11. 结合式信息系统审计方式及适用条件

■ 中国审计学会计算机审计分会《信息系统审计研究报告》课题组编写的《信息系统审计研究报告》，中国时代经济出版社 2015 年出版：

第一部分　总论

第一章　概论

第三节　审计组织方式及其适用条件

一、结合式信息系统审计方式

结合式信息系统审计方式是指在对财政财务及其经济活动的真实性、合法性和效益性审计的同时，对经济活动所依赖的信息系统的安全性、可靠性和经济性进行审计的组织方式。目前，结合式信息系统审计已经成为一种常见的信息系统审计组织方式。结合式信息系统审计在审计计划和审计方案、审计重点、审计程序、审计报告等方面有如下特点。

1. 结合式信息系统审计计划和审计方案

结合式信息系统审计项目计划是伴随财政财务经济活动审计项目计划共同制定的。依据审计项目计划的审计对象、审计期限、审计重点等要素，组织审计项目计划的审计机关统一或分别制订审计工作方案；具体组织审计项目的审计机关依据审计工作方案要求，分别编制经济活动审计项目实施方案、信息系统审计项目实施方案。两个审计项目实施方案在审计对象、审计期限等方面是一致的，在审计重点、审计事项、审计程序和审计方法等方面是不同的。

2. 结合式信息系统审计重点

结合式信息系统审计项目的审计重点，应当按照经济活动审计项目的审计重点和重要审计事项，选择审计关注的经济活动重要事项所依赖的信息系统及其控制，作为信息系统审计的重点，并由此安排审计事项、审计方法和审计人员的配置等。

结合式信息系统审计通常以检查和防范数据风险为审计重点。即：检查和发现信息系统内控缺失可能导致承载业务数据的不真实、不完整、不准确，从而可能带来电子数据审计的“假账真查”风险，为降低电子数据审计的数据风险提供保障。

3. 结合式信息系统审计程序

根据《中华人民共和国国家审计准则》的规定，审计项目的审计程序具体包括审计项目计划、审前调查、审计实施、审计报告、整改跟踪等若干阶段。由于结合式信息系统审计以检查和防范数据风险为重点，需要在审计程序安排上较之于电子数据审计先行一步。即结合式信息系统审计应当依据审计项目计划和审计方案的要求，在审前调查阶段实施并完成重要审计事项的数据风险调查与分析，向综合审计组提出该项目重要审计事项的数据风险审

计报告，为电子数据审计的实施提供数据风险预警；在审计实施阶段，依据审计项目计划和审计方案的相关要求，实施其他内容包括信息系统安全性、可靠性、经济性等方面的审计，并在审计报告阶段出具信息系统审计报告，作为审计项目综合审计报告的重要组成部分。

4. 结合式信息系统审计报告

按照上述审计程序的业务需求，结合式信息系统审计报告包括两类：一是数据风险审计报告。其内容包括：电子数据审计重点关注事项的数据输入、处理、输出的信息系统控制的有效性，揭示系统内控缺失可能导致某类具体数据集的不真实、不完整、不正确，该类内控缺失可能带来对电子数据审计的数据风险，以及对该类数据风险的等级评估，排除数据风险的对策建议等。二是信息系统审计报告。其内容包括：结合数据风险审计报告，重点揭示该类数据风险在管理控制、应用控制、网络控制、安全控制等方面的具体缺失，以及按照审计项目计划和审计方案的其他要求，检查信息系统的安全性、可靠性、经济性，对审计发现的重大问题予以揭示，并提出审计处理意见和审计建议。

■ 庄明来、吴沁红、李俊编写的《信息系统审计内容与方法》，中国时代经济出版社 2008 年出版：

所谓与财务审计相结合的组织方式，是指在财务审计的过程中运用信息系统审计的有关手段进行审计的组织方式。

一般来说，与财务审计相结合的信息系统审计是在财务审计过程中根据财务审计的需要提出的，因此这种信息系统审计应该为减少财务审计的风险服务，为财务审计提供最低限度的保证：（1）保证信息系统软件和相关模块没有经过非法篡改。（2）保证与信息系统相关的内部控制存在并且有效。（3）在财务审计重点关注的领域，应首先进行信息系统审计，以保证信息系统为实现被审计单位的目标服务。与财务审计相结合的组织方式的特点：（1）事先没有专门计划。（2）只是针对部分业务或系统进行信息系统审计。（3）没有专门的信息系统审计报告。

在发生下列情况时，可以考虑采用与财务审计相结合的信息系统审计。

（1）在财务审计之前，审前调查发现被审计单位可能存在信息系统方面的问题。为了减少审计风险，先对信息系统进行审计，然后再针对信息系统薄弱环节，有针对性地进行财务审计。根据审计署计算机技术中心发布的《计算机审计审前调查指南——计算机审计实务公告第 8 号》第十七条的规

定："根据审前调查的初步结果，审计组认为被审计单位所使用的软件或者信息系统可能存在瑕疵或者缺陷，进而可能对于电子数据的真实性、完整性产生重要影响时，应当建议在审计实施方案中增加检查信息系统的内容。"

审计机关和审计组在编制审计实施方案前，应根据审计项目的规模和性质，安排适当的人员和时间，对被审计单位的有关情况进行考察。由于信息技术手段在被审计单位广泛运用，考察的内容还应包括被审计单位所使用的信息系统、电子数据、业务流程对信息化的依赖程度、与信息系统有关的管理机构及管理方式以及开展计算机审计的环境条件等。审前调查的结果表明，如果被审计单位的信息系统及相关方面不存在实质性问题，则可以直接进行数据审计。如果被审计单位的信息系统存在明显错误或缺陷，则需要根据错误和缺陷的具体情况，开展信息系统的审计，减少财务审计的风险。这种根据审前调查结果决定是否进行信息系统审计的方式，是一种以财务审计为主导的方式。在这种方式中，虽然也进行信息系统审计，但信息系统审计最终是为减少财务审计风险服务的。信息系统审计以发现信息系统可能增加财务风险为开始，以通过信息系统审计减少财务审计风险为结束。在这种情况下进行的信息系统审计，一般为对局部模块或单项业务进行的信息系统审计。

（2）在财务审计的过程中，发现一些规律性和倾向性的问题。经初步分析认为，属于信息系统所产生的问题。这个时候应该对相关的信息系统或者模块进行信息系统审计。

财务审计现场审计工作结束后，审计人员对搜集到的审计证据进行整理归纳，这种归纳主要是为总结审计意见，编写审计报告服务。一般来说，现场审计工作进行到此就结束了，但是对于一些经验丰富的审计人员来说，他们往往会发现一些带有规律性和倾向性的问题，特别是当这种问题涉及信息系统的时候，就不能不引起审计人员的高度重视。信息系统作为一种信息自动化处理的手段，当某个问题反复或者频繁出现的时候，就说明信息系统本身出现问题。对于这些规律性或者倾向性的问题，应进行归纳总结，并带着这些问题开展信息系统审计。由于系统开发设计而致使财务信息出现问题并不可怕，怕的是发现问题却不能解决问题。开展信息系统审计，发现问题背后的深层次原因，才是解决问题的根本途径。这种根据财务审计发现问题的规律性特点，进行信息系统审计的方式，表明了信息系统审计开始脱离财务审计的过程，具有一定的独立性。这种情况下进行的信息系统审计，仍然是针对局部模块或单项业务进行的审计，但是整体性和全局性大大加强。事实