中华人民共和国审计署文件

审计发〔2012〕11号

审计署关于印发信息系统审计指南——计算机审计实务公告第34号的通知

各省、自治区、直辖市和计划单列市、新疆生产建设兵团审计厅（局），署机关各单位、各特派员办事处、各派出审计局：

信息系统审计指南——计算机审计实务公告第34号，经署领导同意，现予印发，供审计机关实施信息系统审计参考。

二〇一二年二月一日

信息系统审计指南——计算机审计
实务公告第34号

目　录

第一章　总　则

第一条　为进一步指导和规范国家审计机关组织开展的信息系统审计活动，提高审计效率，保证审计质量，制定本指南。

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。

第三条　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。

第四条　本指南所称审计指标，是指对审计事项的测评指标或者评价指标。

第五条　信息系统审计可以作为财政收支、财务收支及其相关经济业务活动（以下简称经济业务活动）审计项目的审计内容组织开展，也可以作为独立组织的信息系统审计项目实施。

第二章　信息系统审计的组织

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。

第七条　信息系统审计内容，包括对应用控制、一般控制和

项目管理的审计。

应用控制包括：信息系统业务流程，数据输入、处理和输出的控制，信息共享和业务协同。

一般控制包括：信息系统总体控制，信息安全技术控制，信息安全管理控制。

项目管理包括：信息系统建设的经济性，信息系统建设管理，信息系统绩效。

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。

第九条 信息系统审计步骤：

审计机关在开展初选审计项目可行性研究和编制审计实施方案时，要调查了解被审计单位相关经济业务活动及其所依赖的信息系统；

调查了解信息系统的需求与设计、研发与集成、使用与控制、运维与保障等，以及相关的组织架构、责任机制和控制制度；

调查了解系统承载业务的业务流、资金流和信息流，重点分析系统结构和数据结构，标识信息系统审计的关键控制环节和控

制点；

研究并确定信息系统应用控制、一般控制和项目管理的审计内容、审计事项和审计指标；

开展应用控制、一般控制和项目管理的审计测试和评价，获取审计证据，记录相关指标的测评情况，分析系统控制水平以及数据风险，评价系统建设的经济性及信息化投资的有效性；

编写信息系统审计报告。按照审计实施方案要求，依据审计记录和审计证据，评价信息系统的真实性、合法性、效益性和安全性，分析信息系统的控制缺失程度、风险水平、成因和责任，形成审计结论，提出改进信息系统控制、防范系统控制缺失产生审计风险的审计意见和建议。

第十条 结合经济业务活动审计项目组织开展的信息系统审计，可以先实施信息系统控制测评，以便向数据审计提供系统控制缺失产生数据风险的测评结果和审计建议。信息系统审计报告是项目审计报告的重要组成部分。

第十一条 审计人员应当按照审计实施方案确定的审计事项获取相应的审计证据。

获取审计证据的法定权限、程序和方法，以及审计证据的适当性和充分性等，依照审计机关相关规定执行。

第十二条 审计人员应当对能够支持编制审计实施方案和审计报告的相关内容进行审计记录。

审计记录中的调查了解记录、审计工作底稿和重要管理事项

记录，以及与审计证据的关系等，依照审计机关相关规定执行。

第十三条 信息系统审计应当加强审计质量控制。

审计质量控制依照审计机关相关规定执行。

第十四条 信息系统审计中，应当区分各方责任：

在信息系统建设和运维中，遵守国家和行业的相关法律法规和业务规范，建立并实施内部控制以保障经济业务活动的有效运行和组织目标的实现；提供审计机关所需的各类资料和电子数据，并承诺其真实性和完整性，必要时配合审计人员实施系统测试和数据测试，是被审计单位的责任。

信息系统审计中，保守国家秘密和商业秘密，避免对被审计单位信息系统造成损害，以及向审计组提出信息系统控制缺失及其产生数据风险的意见，是审计人员的责任；向审计机关提出审计结果意见，是审计组的责任；向被审计单位提出审计结论、审计意见及建议，是审计机关的责任。

信息系统审计中，审计机关如需利用或者委托具有相关资质的第三方专业机构开展测评的，测评结果的真实性和专业性是第三方专业机构的责任。

第十五条 审计机关依法组织信息系统审计时，有权要求被审计单位对其信息系统配置符合国家或者行业标准的数据接口；在无法配置符合标准的数据接口时，有权要求被审计单位将数据转换成审计机关能够读取的格式并输出；在对电子数据的真实性产生疑问时，有权要求被审计单位按照审计机关提供的方案实施

信息系统的系统测试和数据测试；对被审计单位信息系统不符合法律、法规和政府有关主管部门有关规定的，有权责令限期整改；对故意开发或者使用舞弊功能的单位和个人，有权依法追究其责任。

第十六条 审计机关依法对信息系统的审批、建设、验收、运维等特定事项，向有关部门或者单位进行专项审计调查。

专项审计调查依照审计机关相关规定执行。

第十七条 审计机关在依法实施的信息系统审计中发现影响国家信息安全的重大问题，应当向相关主管部门专题报告或者移送。

专题报告或者移送依照审计机关的相关规定执行。

第十八条 审计人员应当具备信息系统审计的基本知识和技能。实施信息系统审计的审计组成员中，应当配备具有信息系统审计专业知识和技能的审计人员。必要时可聘请外部专家或者委托专业机构开展专项检查和评价。

聘请外部专家或者委托专业机构开展工作，依照审计机关相关规定执行。

第三章 应用控制审计

第一节 信息系统业务流程控制审计

第十九条 信息系统业务流程控制审计的目的是通过检查被

审计单位信息系统承载的经济业务活动的发生、处理、记录和报告的业务流程和业务循环过程，评价系统业务流程控制的合理性和有效性，揭示系统业务流程设计缺陷、控制缺失等问题，形成审计结论，提出审计意见和建议；为防范和控制数据审计风险，以及审计项目对信息系统业务流程控制的审计评价提供支持。

第二十条 信息系统业务流程控制审计事项测评指标：

（一）业务流程设计测评。检查业务流程设计的完备性，是否满足经济业务活动的需求，是否实施了业务流程整合、还原或者再造，是否避免了重复操作，关键环节、关键节点和关键岗位是否具备不相容职责分离等必要的控制。

（二）业务流程处理测评。检查系统业务处理的正确性和控制的有效性，各流程节点的操作是否反映了经济业务活动的审批及处理过程要求，是否设置了相同业务处理的自动批量操作，是否对重要的业务流程处理实施了有效的控制和校验，接口处理是否正确，控制是否有效等。

（三）业务流程功能测评。检查系统业务流程实现功能的合理性，各类功能操作是否能够满足经济业务活动的需要，问题管理、应急处理和系统控制等功能是否有效。

第二节 数据输入、处理和输出控制审计

第二十一条 数据输入、处理和输出控制审计的目的是通过检查被审计单位信息系统数据输入、处理和输出控制的有效性，发现因系统控制缺失产生的数据风险，形成数据控制水平的审计

评价和结论，提出审计意见和建议；为数据审计防范和控制审计风险，以及审计项目对信息系统数据风险控制的审计评价提供支持。

第二十二条 审计人员应当在调查了解被审计单位信息系统所承载的经济业务活动的业务流、资金流和信息流基础上，按照不同经济业务活动的数据输入、处理和输出功能，分类建立测评指标，开展测评和审计分析。

第二十三条 数据输入控制审计事项测评指标：

（四）数据录入和导入控制测评。检查系统有无设置不符合国家、行业或者单位规范的数据录入、导入接口等数据采集功能，数据采集的身份与权限控制是否合理、有效。

（五）数据修改和删除控制测评。检查系统有无设置不符合国家、行业或者单位规范的数据修改或者删除功能，用户数据修改和删除等身份与权限控制是否合理、有效。

（六）数据校验控制测评。检查数据录入、导入接口等数据采集功能的校验控制是否符合国家、行业或者单位的规定，校验控制是否有效。

（七）数据入库控制测评。检查录入、导入接口等采集的数据、缓冲区数据与进入数据库的最终数据是否一致。

（八）数据共享与交换控制测评。检查系统有无设置不符合国家、行业或者单位规范的数据共享与交换功能，用户或者系统的数据共享与交换的身份与权限控制是否合理、有效。

（九）备份与恢复数据接收控制测评。检查数据备份与恢复的数据接收功能的身份与权限控制是否合理、有效，接收数据与输出数据是否一致。

第二十四条 数据处理控制审计事项测评指标：

（十）数据转换控制测评。检查系统采集外部数据和转换过程中的各项控制，是否符合国家、行业或者单位的数据转换标准和格式规范。

（十一）数据整理控制测评。检查采集数据的分类入库、数据库中相关数据的清洗、数据库间和数据表间的数据抽取与合并、数据库或者数据表的生成与废除等功能的控制，是否符合系统需求和设计要求。

（十二）数据计算控制测评。检查系统中经济业务活动的计量、计费、核算、分析，以及数据勾稽、数据平衡、断号重号等计算功能的控制，是否符合国家、行业或者单位的相关规定和规范。

（十三）数据汇总控制测评。检查系统中经济业务活动的财政财务科目汇总、报表汇总和相关业务汇总等功能实现的控制，是否符合国家、行业或者单位的相关规定和规范。

第二十五条 数据输出控制审计事项测评指标：

（十四）数据外设输出控制测评。检查计算机显示、打印和介质拷贝等数据输出功能的身份与权限控制。

（十五）数据检索输出控制测评。检查利用单项检索、组合

检索等检索工具对系统中部分数据或者全部数据的检索输出功能的身份与权限控制。

（十六）数据共享输出控制测评。检查系统内部相关子系统之间、系统与外部系统之间通过信息交换或者信息共享方式数据输出功能的身份与权限控制。

（十七）备份与恢复输出控制测评。检查运行系统向备份系统、备份系统向恢复系统数据输出的身份与权限控制是否合理、有效。

第三节　信息共享和业务协同审计

第二十六条　信息共享与业务协同审计的目的是通过检查被审计单位信息系统内外部信息共享与业务协同，揭示共享与协同控制的缺失，分析并评价风险程度，形成被审计单位信息共享与业务协同水平的审计评价和结论，提出审计意见和建议；为数据审计获取真实、完整和正确的审计数据，以及审计项目对被审计单位信息共享与业务协同的审计评价提供支持。

第二十七条　信息共享与业务协同审计事项测评指标：

（十八）信息资源目录体系测评。检查信息资源目录体系是否符合国家或者行业的相关规范，是否较好地满足各类业务和管理的需要。

（十九）信息资源交换体系测评。检查信息资源交换体系是否符合国家或者行业的相关规范，是否较好地满足信息交换的需要。

（二十）元数据和主数据测评。检查系统中的元数据和主数据是否符合国家、行业或者单位的相关规范，是否较好地满足信息系统建设、应用和共享的需要。

（二十一）数据元素和数据库表测评。检查系统中的数据元素（数据库表中的数据字段）和数据库表，是否符合行业或者单位的相关规范，是否较好地满足信息系统建设、应用和共享的需要。

（二十二）内部数据和外部数据测评。检查信息系统内部产生的包括预算管理、会计核算和相关业务的数据，以及为履行职能或者实现经济业务活动需要从其他单位获取的外部数据，形成的各类数据是否具有真实性、完整性和正确性，是否较好地满足经济业务活动的需要。

（二十三）信息资源标准化测评。检查信息系统是否建立了满足信息共享和业务协同的信息资源标准和规范，是否执行了国家或者行业的标准化要求，是否为推进经济业务活动的共享协同提供了有效支撑。

第二十八条 共享信息建设审计事项测评指标：

（二十四）公共基础信息建设测评。检查被审计单位按照国家或者行业确定的人口、法人、空间地理等满足公共需要的公共基础信息的建设任务，是否按照国家或者行业关于公共基础信息的标准规范组织建设，是否建立了公共基础信息共享的管理制度和机制，是否具有较为完备的信息系统实现功能，是否支持了公

共基础信息的信息共享与业务协同。

（二十五）其他共享信息建设测评。检查被审计单位按照国家或者行业确定、或者与其他部门协定的满足其他部门经济业务活动需要的共享信息的建设任务，是否按照国家、行业或者协定的共享信息标准规范组织建设，是否建立了共享信息的管理制度和机制，是否具有较为完备的信息系统实现功能，是否支持了其他部门的信息共享与业务协同。

（二十六）信息共享平台建设测评。检查被审计单位按照国家或者行业确定的信息共享平台建设任务，是否按照国家或者行业关于共享平台建设的标准规范组织建设和运维，是否建立了信息共享和信息安全的技术控制和管理机制，是否具有较为完备的信息系统实现功能，是否支持了相关部门的信息共享和业务协同。

第二十九条 共享外部数据审计事项测评指标：

（二十七）共享外部数据测评。检查被审计单位职能需要的公共基础信息和其他共享信息，以及与系统内部数据的业务关联度，是否具有较为明确的共享外部数据信息目录和格式规范。

（二十八）共享外部数据有效性评估。检查被审计单位是否建立了获取外部数据的相关制度和机制，系统是否具有获取外部数据的接口功能，分析外部数据缺失对被审计单位经济业务活动有效性的影响，分析研究缺失外部数据的原因和解决途径。

第三十条 供给外部数据审计事项测评指标：

（二十九）供给外部数据测评。检查系统是否具有外部所需

的公共基础信息和其他共享信息，是否建立了供给外部数据和信息资源共建共享的相关制度和机制，是否能够满足外部政务职能、社会管理职能等组织机构的信息需求。

（三十）供给外部数据有效性评估。检查被审计单位是否建立了供给外部数据的相关制度和机制，系统是否具有符合国家或者行业数据接口标准的数据输出接口功能，是否按照国家或者行业相关规定实现了有效的信息交换与共享机制，是否较好地支持了外部系统相关业务的协同发展。

第四章　一般控制审计

第一节　信息系统总体控制审计

第三十一条　信息系统总体控制审计的目的是通过检查被审计单位信息系统总体控制的战略规划、组织架构、制度机制、岗位职责、内部监督等，分析信息系统在内部环境、风险评估、控制活动、信息与沟通、内部监督方面的有效性及其风险，形成信息系统总体控制的审计评价和结论，提出审计意见和建议，促进信息系统总体控制的完善，并为审计项目对信息系统总体控制的审计评价提供支持。

第三十二条　信息系统总体控制审计事项评价指标：

（三十一）战略规划评价。检查被审计单位是否建立了信息系统战略发展规划，是否明确了战略目标、整体规划、实现指标

和相应的实施机制，以及规划的业务和管理的覆盖面、所辖行业的覆盖面，是否能够指导和推进信息化环境下经济业务活动的战略发展。

（三十二）组织架构评价。检查被审计单位是否建立了与信息系统战略发展规划相匹配的决策与管理层领导机构、项目实施层工作机构，以及行业内各层级的信息化工作机构，是否建立了各类机构的权力责任和制约机制，是否有效地发挥了各类机构的作用。

（三十三）制度体系评价。检查被审计单位是否建立了与信息系统战略规划和组织架构相匹配的项目管理制度、项目建设制度、质量检查制度等，是否建立了重大问题的决策机制，是否形成了领导机构对项目实施机构和行业工作机构的统一领导，项目实施机构是否形成了对项目建设进度、项目质量、投资效果和风险防范的有效控制。

（三十四）岗位职责评价。检查被审计单位信息系统规划、建设、运维等方面的岗位设置、人员配置、岗位职责，是否建立了各类岗位职责的检查考核机制，是否建立了信息系统建设和经济业务活动之间、信息系统建设的相关岗位之间有效的信息沟通与交互机制。

（三十五）内部监督评价。检查被审计单位是否建立健全了信息系统建设和运维全过程的内部监督机构和监督机制，是否形成了对信息系统的风险评估、控制活动和信息交互等方面的有效

控制和监督，是否较好地发挥了促进信息系统健康运行的监督保障作用。

第二节　信息安全技术控制审计

第三十三条　信息安全技术控制审计的目的是通过检查被审计单位信息系统的信息安全技术及其控制的整体方案，检查安全计算环境、区域边界、通讯网络等方面的安全策略和技术设计，检查信息系统的安全技术配置和防护措施，发现并揭示信息系统安全技术控制的缺失，分析并评价风险程度，形成信息安全技术控制的审计结论，提出审计意见和建议，促进信息系统安全技术及其相关控制的落实；为数据审计防范和控制审计风险，以及审计项目对信息安全技术控制的审计评价提供支持。

第三十四条　信息安全技术控制审计事项测评指标：

（三十六）物理安全控制测评。检查系统机房及其重要工作房间的物理位置选择、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、电磁防护等方面的安全策略和防护措施。

（三十七）网络安全控制测评。检查网络结构安全、网络设备访问控制、网络设备安全审计、网络边界完整性、网络入侵防范、网络恶意代码防范、网络设备防护的安全策略和防护措施。

（三十八）主机安全控制测评。检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的身份鉴别、访问控制、安全审计和剩余信息保护方面的安全策略和防护措施，检查主要

服务器的入侵防范、恶意代码防范和资源控制措施。

（三十九）应用安全控制测评。检查主要应用系统的身份鉴别、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、软件容错和资源控制等方面的安全策略和防护措施。

（四十）数据安全控制测评。检查主要系统管理数据、鉴别信息和重要业务数据的完整性、保密性、备份和恢复方面的安全策略和防护措施。

（四十一）信息化装备自主可控测评。检查信息系统在网络、主机、安全、系统软件和应用软件等信息化装备的自主可控情况，检查是否能够促进信息系统内外结合的安全防护，保障信息系统运行安全。

第三节　信息安全管理控制审计

第三十五条　信息安全管理控制审计的目的是通过检查被审计单位信息系统的信息安全管理，评价信息安全管理的完整性和有效性，揭示信息安全管理缺失的问题，形成信息安全管理控制的审计评价和结论，提出审计意见和建议，促进信息系统安全管理的有效性；为数据审计防范和控制审计风险，以及审计项目对系统安全管理的审计评价提供支持。

第三十六条　信息安全管理控制审计事项评价指标：

（四十二）安全管理机构评价。检查安全管理机构是否健全，检查岗位设置、人员配备、授权和审批、沟通和合作、审核和检

查等情况。

（四十三）安全管理制度评价。检查安全管理制度体系是否包含总体方针、安全策略、管理制度、操作规程等文件，是否覆盖物理、网络、主机、应用和数据的建设及管理等内容，检查安全管理制度的制定、评审、发布、修订和实施等情况。

（四十四）人员安全管理评价。检查人员录用、人员离岗、人员考核、安全意识教育和培训、外部人员访问管理等情况。

（四十五）系统建设安全管理评价。检查信息系统的安全定级、安全方案设计、产品采购和使用、软件的自行开发与外包开发、工程实施、测试验收、系统交付、系统安全备案和安全服务商选择等情况。

（四十六）系统运维安全管理评价。检查环境管理、资产管理、介质管理、设备管理、监控管理、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、应急预案管理等情况。系统运维采用第三方外包方式的，要重点检查第三方运维管理是否有利于系统运维安全，是否存在影响信息系统安全性方面的问题。

第五章　项目管理审计

第一节　信息系统建设经济性评价

第三十七条　信息系统建设经济性审计的目的是通过检查

被审计单位信息系统规划、建设、应用和运维的经济性，发现系统建设不经济的问题，形成审计结论，提出审计意见和建议，促进信息化建设投资的有效性，并为审计项目对信息系统建设经济性的审计评价提供支持。

第三十八条 信息系统规划经济性审计事项评价指标：

（四十七）总体规划经济性评价。检查信息系统是否进行了总体规划，是否按照职能需求实施了总体目标、分期建设目标和考核指标的整体设计，顶层设计总体框架是否具备业务发展的可扩展性、信息系统的可持续性、系统应用对经济社会发展的效益性。重点检查信息系统及其各子系统的生命周期，评价总体规划的经济性。

（四十八）业务整合规划经济性评价。检查信息系统是否按照组织目标和职能业务特征要求进行了业务和管理的流程再造、信息共享、系统功能整合与复用等方面的整合规划，避免信息孤岛和投资浪费。

（四十九）行业整合规划经济性评价。检查信息系统是否按照行业信息化特征要求进行了统一规划、统一建设、推广应用、信息共享和业务协同，是否有效避免本行业同类业务的重复建设和重复投资。

（五十）技术特征规划经济性评价。检查被审计单位按照经济业务活动对信息系统运行的不可间断性、并发性和系统响应速度，以及数据存储量、传输量和处理量等方面的技术特征需求，

进行的主机、网络、安全、应用等技术架构和技术装备性能配置方面的规划设计，是否具有合理性、经济性和有效性，避免技术装备性能过度冗余和投资浪费。

第三十九条 信息系统建设经济性审计事项评价指标：

（五十一）建设规划经济性评价。检查分期建设的信息系统是否按照总体规划要求较好地实施了业务整合、管理整合及其行业应用整合，技术架构和技术性能装备配置是否具有合理性、经济性和有效性，系统建设投资是否合理。

（五十二）招标采购经济性评价。检查是否按照建设规划进行了利用原有信息资产和新购技术装备的整体规划，是否较好地实施了招标采购项目的业务需求和技术方案论证，招标采购的工程、设备和服务是否体现了满足业务需求、支持自主可控、技术先进适用和合理性价比的要求。

（五十三）应用开发经济性评价。检查应用系统开发是否结合单位职能、业务和管理特征，采用适合的应用系统开发方法，采取功能复用、标准化、可扩展、可移植等设计与开发策略，增强应用系统效用性，延长应用系统生命周期，提高投资效果。

（五十四）应用推广经济性评价。检查是否结合本行业业务和管理的信息化特征，采取相适应的应用系统推广和集约化部署策略，增强部门系统建设拉动行业应用的经济性。

第四十条 信息系统应用经济性审计事项评价指标：

（五十五）业务管理对信息系统的依赖度评价。检查分析现

有业务和管理尤其是核心业务对信息系统的依赖程度，评价信息系统建设投资的必要性。

（五十六）信息系统对业务管理的支持度评价。检查分析信息系统对现有业务和管理的运行，以及对业务和管理预期发展的技术支持等方面的作用，评价信息系统建设投资的必要性。

（五十七）系统应用对提升效能的贡献率评价。检查分析信息系统应用对提升业务和管理的运行效率和效能，促进业务和管理的组织方式实现，促进信息化环境下履职能力的提高，从而促进职能对象状况的改变，以及对其他行业信息化建设和应用的影响等。

第四十一条 信息系统运维经济性审计事项评价指标：

（五十八）信息系统运维经济性评价。检查分析信息系统运维总投资与信息系统建设总投资的占比，评价信息系统运维的经济性。

（五十九）信息资产运行经济性评价。检查分析系统建设形成的信息资产总价值与信息系统建设总投资的占比、在线运行信息资产价值与信息资产总价值的占比，评价信息资产运行的经济性。

（六十）信息资产运维经济性评价。检查分析信息资产运维投资与信息资产总价值的占比，评价信息资产运维的经济性。

第二节 信息系统建设管理评价

第四十二条 信息系统建设管理审计的目的是通过检查被

审计单位信息系统建设的立项申报、建设管理、资金管理、监督管理、验收管理、运行管理、等保管理和风险评估管理，揭示系统建设管理控制缺失的问题，提出审计意见和建议，促进项目建设管理的规范性，为审计项目对信息系统建设管理的审计评价提供支持。

第四十三条 项目审批管理审计事项评价指标：

（六十一）项目立项规划评价。检查立项申请是否符合国家或者行业有关规定和规划要求。

（六十二）项目建议书评价。检查项目建设单位编制的需求分析报告和项目建议书，是否通过了有相应资质专业机构的评估，并获得审批部门批复。

（六十三）项目可行性研究报告评价。检查可行性研究报告是否招标选定或者委托具有相关资质的工程咨询机构或者设计单位编制，是否通过了有相应资质机构的评估，并获得审批部门批复。

（六十四）项目初步设计评价。检查初步设计方案和投资概算报告是否招标选定或者委托具有相关资质的设计单位编制，是否通过了有相应资质机构的评估，并获得审批部门批复。

（六十五）项目调整审查评价。检查项目建设过程中的建设内容和投资概算有较大变动时，是否按照规定程序向项目审批部门报送调整报告并经批准；项目建设过程中出现工程严重逾期、投资重大损失等问题时，是否及时向项目审批部门报告。

第四十四条 项目建设管理审计事项评价指标：

（六十六）项目管理评价。检查项目建设单位是否确定实施机构和责任人，是否建立健全管理制度，是否按规定向项目审批部门报告有关实施情况。

（六十七）项目招标采购评价。检查项目是否按国家规定组织了招标投标和政府采购，项目设计、施工、研发、集成等单位是否符合规定的资质，采购的各类软硬件、产品厂商和供应商是否符合相关规定，是否较好地实施了自主可控信息化装备优先采购的策略，有无发生招标纠纷，纠纷解决措施是否得当。

（六十八）项目合同内容与执行情况评价。检查项目合同建设内容、合同价格、软件版权归属、不可抗力因素和法律纠纷对策等方面的合法性，项目建设内容的交付是否符合合同约定，资金支付进度、程序和方式是否符合合同约定和国家有关规定。

（六十九）项目监理情况评价。检查项目是否执行了国家规定的项目监理制度，是否实行了项目方、设计方、施工方、集成方和监理方的制约机制，是否监督了监理方严格履行职责，是否保障了项目确定的质量、进度和投资。

（七十）项目建设方式评价。检查项目实行外包建设和自行建设等不同方式的合理性和有效性，重点检查自行建设的合法性。

第四十五条 项目资金管理审计事项评价指标：

（七十一）项目支出预算评价。检查项目建设单位是否按项目实施进度和相关规定向项目审批部门和财政部门提出年度资金

使用计划、政府采购预算等申请。

（七十二）项目支出核算评价。检查项目建设单位的资金使用、会计核算、项目决算等是否符合项目批复和国家有关规定。

（七十三）项目审计情况评价。检查项目的审计情况，审计报告提出的问题是否得到有效整改。

第四十六条 项目监督管理审计事项评价指标：

（七十四）项目监督审查配合评价。检查项目建设单位在接受项目审批部门及其财政、审计等有关部门的监督检查时是否如实提供建设项目有关的资料和情况，有无拒绝、隐匿、瞒报等情况。

（七十五）项目监督审查整改评价。检查项目建设单位对有关部门监督检查提出的问题和处理意见是否进行了积极整改，整改后的情况是否符合相关规定。

第四十七条 项目验收管理审计事项评价指标：

（七十六）项目单项验收和初步验收评价。检查项目建设单位是否按规定及时组织单项验收，是否在项目建设完成后的规定时间内组织初步验收，各项验收是否符合相关规定。

（七十七）项目竣工验收评价。检查项目建设单位是否按照有关规定向项目审批部门提出竣工验收申请，未按期完成的是否提出延期竣工验收申请，项目是否通过竣工验收和批复。

（七十八）项目后评估整改评价。检查项目建设单位是否接受了项目主管部门组织的后评估，对后评估中提出的系统运行效

率、使用效果等问题是否进行了及时有效整改，有无拒不整改或者整改后仍不符合要求的情况。

第四十八条 项目运行管理审计事项评价指标：

（七十九）项目运行管理评价。检查项目建设单位是否落实了项目运行管理机构和管理人员，是否实行了运行管理责任制，是否制定和完善了管理制度。

（八十）项目运维服务评价。检查项目建设单位是否建立了有效的运维服务队伍和机制，落实了运维服务资金，加强了日常运行和维护管理，保障了信息系统运行的可靠性。

第四十九条 涉密信息系统分级保护审计事项评价指标：

（八十一）涉密信息系统定级审批评价。检查涉密信息系统是否在建设前通过了主管部门的分级保护定级的审核批准。

（八十二）涉密信息系统使用审批评价。检查涉密信息系统是否在建成后通过了主管部门的安全保密测评和投入使用的审核批准。

（八十三）涉密信息系统整改与备案评价。检查已投入使用的信息系统是否完成系统整改后向主管部门备案。

第五十条 非涉密信息系统等级保护审计事项评价指标：

（八十四）等级保护备案审批评价。检查非涉密信息系统是否在建设前向主管部门备案定级情况并得到审核批准。

（八十五）等级保护测评情况评价。检查非涉密信息系统是否在建成后通过了主管部门组织的等级保护测评。

（八十六）等级保护自查整改评价。检查非涉密信息系统是否在投入使用后按规定组织自查，并依据主管部门检查意见进行整改。

第五十一条 信息安全风险评估审计事项评价指标：

（八十七）风险评估委托测评评价。检查项目是否按规定委托有资质的测评机构进行了风险评估。

（八十八）风险评估整改落实评价。检查是否对信息安全风险评估报告提出的整改意见予以落实。

（八十九）残余风险评估与防范评价。检查对残余风险是否采取了相应的防范措施。

第三节 信息系统绩效评价

第五十二条 信息系统绩效评价的目的是通过检查被审计单位信息系统顶层设计及建设实现的管理决策支持能力、经济业务协同能力、系统建设发展能力和信息系统贡献能力的提升，以及经济业务活动的效率、效果和效能的改善，揭示信息系统顶层设计和建设方面的不足，提出审计意见和建议，进一步促进信息系统的实际效能提升，为审计项目对系统建设绩效的审计评价提供支持。

第五十三条 信息系统绩效审计事项评价指标：

（九十）信息系统总体绩效评价。检查信息系统的规划目标、发展战略、创新策略、分期建设方案和考核指标等，评价总体规划和分期建设方案对信息系统实际建设和应用的指导性效能的影

响程度。

（九十一）管理决策支持能力的绩效评价。检查信息系统对支持和提升组织管理、业务管理、行政管理等方面的情况，评价信息系统对提升管理决策能力，改善经济业务发展方面的效率、效果与效能的影响程度。

（九十二）信息资源共享能力的绩效评价。检查信息系统中的管理资源、业务资源、人力资源、财力资源、技术资源、市场资源等各类信息资源的共享程度和利用状况，评价信息系统的共享协同对改善经济业务发展的效率、效果与效能的影响程度。

（九十三）经济业务协同能力的绩效评价。检查信息系统对提升单位内部不同业务之间、行业内部不同单位之间、与外部相关经济业务之间的业务协同情况，评价信息系统对提升经济业务协同能力，改善经济业务发展的效率、效果与效能的影响程度。

（九十四）系统建设发展能力的绩效评价。检查信息系统的整体架构、技术路线、开发策略、应用模式和运维模式，以及应对职能业务发展、信息技术发展、环境风险防范等方面的适应能力，评价信息系统对职能业务发展可持续支持的影响程度。

（九十五）信息系统贡献能力的绩效评价。检查信息系统运行对单位经济业务活动和国家经济社会健康发展的经济效益、社会效益的影响，信息系统的规划模式、建设模式等对其他行业信息化的可借鉴性，评价信息系统对经济业务发展和行业、地区信息化发展的贡献度。

第六章　信息系统审计方法

第五十四条　系统调查方法。依据审计实施方案确定的审计目标和审计事项，调查被审计单位的相关业务活动及其所依赖的信息系统，调查信息系统的立项审批、系统建设、运行管理、运维服务、项目投资等情况，以及相关责任机构和管理制度等。

第五十五条　资料审查方法。为了确定信息系统的重要控制环节和重要控制点，审查信息系统的立项审批、系统设计、招标采购、项目实施、项目验收、系统运行、运维服务、项目投资，以及各类第三方测试或者评估等相关文档资料。重点审查应用控制、一般控制和项目管理中的重要事项资料。

第五十六条　系统检查方法。为了核定信息系统的重要控制环节和重要控制点，需要对应用控制的数据输入、处理、输出及其信息共享与业务协同的相关控制进行检查，对一般控制环境、区域边界和网络通信，以及信息系统的物理环境、网络、主机、应用、数据和安全等各类系统控制进行实地检查。

第五十七条　数据测试方法。为验证数据输入、处理和输出控制的有效性，采用模拟数据对运行系统或者备份系统进行符合性测试；对重要的计量、计费、核算、分析等计算功能及其控制进行设计文档审查、系统设置检查和数据实质性测试的审查。必要时审查应用系统的源程序等。

第五十八条　数据验证方法：

数据采集验证。利用直连式、旁路式、代理式等合适的数据

采集方法和工具，采集系统监测日志或者相关业务数据，进行数据符合性验证。

数据转换验证。利用数据库数据转换、文本转换、网页信息转换等方法和工具，对异构数据库之间的数据转换、结构化数据和非结构化数据的转换、不同数据类型和格式之间数据转换的一致性和准确性进行检查验证。

数据处理验证。通过对数据库 SQL 语句进行转换解析，实现对各类经济业务活动的计量、计费、核算、汇总等计算的符合性与准确性进行验证。

第五十九条 工具检测方法：

安全工具检测。利用入侵检测、漏洞扫描等工具的监测结果进行分析评价。

审计工具检测。利用网络审计、主机审计、数据库审计等工具的日志记录结果进行分析评价。

测评工具检测。利用网络分析检测、系统配置检测、日志分析检测等工具，通过采集信息系统之间的通信数据包并进行逆向分析，还原系统间通信内容，检测主机操作系统、数据库、网络设备等重要系统是否满足配置标准和规范要求，采集操作系统、网络设备、安全设备、应用系统等生成的日志信息进行检测分析。

系统运行监测。利用网络流量、应用进程、CPU 利用率、内存利用率等系统运行监测结果进行分析评价。

系统监控检测。利用对应用、数据、主机、网络、机房环境

设备设施等方面的系统运行监控记录进行分析评价。

第六十条 风险评估方法：

信息系统内外部风险评估。在对信息系统总体风险的评估中，要充分考虑被审计单位信息系统及其经济业务活动所面临的国内外经济环境、政策影响、市场影响、技术影响、文化影响和组织架构影响等因素，以便做出客观的评价。

信息系统控制缺失风险评估。对检查测评发现的系统各类控制缺失应当进行风险程度评估，区分可接受的风险和不可接受的风险，尤其要重视潜在风险的评估。

控制缺失导致业务数据风险的评估。对检查测评发现的控制缺失不可接受的风险，要对是否导致经济业务活动相关数据的风险进行评估，指出具有风险的数据库和数据表，评估数据风险的程度。

信息系统风险责任界定评估。按照固有风险、控制风险和检查风险的审计风险理论，对信息系统的设计与建设、运行与维护、检查与监督等各环节的风险进行评估，对各部门的责任进行界定。

第六十一条 专家评审方法。组织信息系统等相关方面的专家或者委托有资质的专业机构，对信息系统审计中的相关专业领域、关键技术等进行必要的评审。

第七章 附 则

第六十二条 本指南适用于国家审计机关组织开展的各类信

息系统审计活动。

第六十三条 本指南的审计内容和审计指标，均依照国家关于信息系统建设和管理的相关规定，参照国内外信息系统审计的研究成果，在总结我国审计机关信息系统审计实践的基础上提出。

第六十四条 本指南的审计事项、审计指标和审计方法，需要在审计实践中不断完善、调整和扩充，逐步建立适合我国国家审计机关的信息系统审计指标体系和审计方法体系。

第六十五条 本指南由中国审计学会计算机审计分会、审计署信息化建设办公室、审计署计算机技术中心、审计署科研所、审计署外资审计中心，审计署京津冀特派员办事处、上海特派员办事处、南京特派员办事处、武汉特派员办事处、长沙特派员办事处，浙江省审计厅，南京审计学院、北京大学数字中国研究院等单位起草。

第六十六条 本指南的解释权属审计署计算机技术中心。

第六十七条 本指南自发布之日起生效。

附录

信息系统中容易产生数据风险的审计内容

1．第二十条信息系统业务流程控制审计事项的（一）至（三）测评指标。

2．第二十三条至第二十五条的数据输入、处理和输出审计事项的（四）至（十七）测评指标。

3．第二十七条信息共享与业务协同控制审计事项的（十八）、（二十）至（二十二）测评指标。

4．第二十九条共享外部数据审计事项的（二十七）测评指标，第三十条供给外部数据审计事项的（二十九）测评指标。

5．第三十四条信息安全技术控制审计事项的（三十七）、（三十八）至（四十）测评指标。

主题词：审计　计算机　公告　通知

署内分送：署领导，总经济师，办公厅、计算中心（4）。

审计署办公厅　　2012 年 2 月 2 日印发

（只发电子文件）