 第一章总则 第一条为了规范组织内部审计机构及人员开展信息系统审计活动，保证审计质量，根据《内部审计基本准则》制定本准则。 第二条本准则所称信息系统审计，是指由组织内部审计机构及人员对信息系统及其相关的信息技术内部控制和流程开展的一系列综合检查、评价与报告活动。 第三条本准则适用于各类组织的内部审计机构、内部审计人员及其从事的信息系统审计活动。 第二章一般原则 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，对组织是否达成信息技术管理目标进行综合评价，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其受托责任以达成组织的信息技术管理目标。组织的信息技术管理目的是保证组织的信息技术战略充分反映该组织的业务战略目标，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，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及监管的相关要求。 第五条组织中信息技术管理人员的责任是信息系统的开发、运行和维护以及信息技术相关的内部控制的设计、执行和监控；信息系统审计人员的责任是实施信息系统审计工作并出具审计报告。 第六条从事信息系统审计人员的专业胜任能力是指在信息系统审计领域,胜任管理层与其他利益方的委托、履行其信息系统审计职能所应拥有的相关知识、技能和素质。信息系统审计人员应当熟悉内部审计业务并具备必要的信息技术及信息系

统审计的专业知识。此外，审计项目负责人员应具有三年以上信息系统审计相关工作经验，或六年以上相关业务的从业经验。由于组织特殊性而产生的例外情况，应当获得组织管理层的特别授权。组织应当建立信息系统审计人员培训制度，鼓励审计人员取得注册信息系统审计师等执业资格，以保证审计人员的专业胜任能力。必要时，信息系统审计可利用外部专家的服务。 第七条信息系统审计可作为独立的审计项目组织实施、或作为综合性内部审计项目的组成部分实施。第八条信息系统审计划分为以下阶段：审计计划阶段、审计实施阶段、审计报告与后续工作阶段。 第九条审计人员应采用以风险为导向的审计方法进行信息系统审计，风险评估应贯穿审计的计划、实施、报告与后续工作各个阶段。 第三章 审计计划 第十条内部审计人员在执行信息系统审计之前，需要确定审计目标并初步评估审计风险，估算完成信息系统审计或专项审计所需的资源，确定重点审计领域及审计活动的优先次序，明确审计组成员的职责，并以此制定信息系统审计计划。 第十一条制定信息系统审计计划时，应遵循其他相关内部审计具体准则规定的因素，同时针对信息系统审计的特殊性，审计人员还应充分考虑以下因素：（一）高度依赖信息技术、信息系统的关键业务流程及相关的组织战略目标；（二）信息技术管理的组织架构；（三）信息系统框架和信息系统的长期发展规划及近期发展计划；（四）信息系统及其支持的业务流程的变更情况；（五）信息系统的复杂程度；（六）以前年度信息系统内、外部审计等相关的审计发现及后续审计情况。 第十二条信息系统审计作为综合性内部审计项目的一部分时，审计人员在审计计划阶段还应综合考

虑相关内部审计的审计目标及要求。 第四章信息技术风险评估 第十三条进行信息系统审计时，审计人员应当识别组织所面临的与信息技术相关的内、外部风险，并采用适当的风险评估技术与方法，分析及评价其发生的可能性及影响程度，为确定审计目标、范围和方法提供依据。 第十四条信息技术风险是指组织在信息处理和信息技术运用过程中产生的、可能影响组织目标实现的各种不确定因素。信息技术风险包括组织层面的信息技术风险、一般性控制层面的信息技术风险及业务流程层面的信息技术风险等。 第十五条审计人员在识别、评估组织层面、一般性控制层面的信息技术风险时需要关注以下几方面：（一）业务关注度，即组织的信息技术战略与组织整体发展战略规划的契合度以及信息技术（包括硬件及软件环境）对业务和用户需求的支持度；（二）信息资产的重要性；（三）对信息技术的依赖程度；（四）对信息技术部门人员的依赖程度；（五）对外部信息技术服务的依赖程度；（六）信息系统及其运行环境的安全性、可靠性；（七）信息技术变更；（八）法律规范环境；（九）其他。第十六条业务流程层面的信息技术风险受行业背景、业务流程的复杂程度、上述组织层面及一般性控制层面的控制有效性等因素的影响而存在差异。一般而言，审计人员应了解业务流程并关注以下几方面信息技术风险：（一）数据输入；（二）数据处理；（三）数据输出。 第十七条审计人员应充分考虑风险评估的结果，以合理确定信息系统审计的内容及范围，并对组织的信息技术内部控制的设计有效性和执行有效性进行测试。 第五章信息系统审计的内容 第十八条信息系统审计通常包括对组织层面信息技术控制、信息技术一般性

控制及业务流程层面相关应用控制的审计。 第十九条信息技术内部控制的各个层面都包括人工控制、自动控制和人工、自动相结合的控制形式，审计人员应根据不同的控制形式采取恰当的审计程序。 第二十条组织层面信息技术控制是指管理层及治理层对信息技术治理职能及内部控制的重要性的态度、认识和措施，审计人员应考虑以下控制要素中与信息技术相关的内容：（一）控制环境 审计人员应关注该组织的信息技术战略规划对业务战略规划的契合度、信息技术治理制度体系的建设、信息技术部门的组织结构和关系、信息技术治理相关职权与责任的分配、信息技术人力资源管理、对用户的信息技术教育和培训等方面；（二）风险评估 审计人员应关注组织的风险评估的总体架构中信息技术风险管理的框架、流程和执行情况、信息资产的分类以及信息资产所有者的职责等方面；（三）信息与沟通 审计人员应关注组织的信息系统架构及其对财务、业务流程的支持度、管理层及治理层的信息沟通模式、信息技术政策/信息安全制度的传达与沟通等方面；（四）监控 审计人员应关注组织的监控管理报告系统、监控反馈、跟踪处理程序以及组织对信息技术内部控制的自我评估机制等方面。 第二十一条信息技术一般性控制是指与网络、操作系统、数据库、应用系统及其相关人员有关的信息技术政策和措施，以确保信息系统持续稳定的运行，支持应用控制的有效性。对信息技术一般性控制的审计应考虑以下控制活动：（一）信息安全管理 审计人员应关注组织的信息安全管理政策，物理访问及针对网络、操作系统、数据库、应用系统的身份认证和逻辑访问管理机制，系统设置的职责分离控制等；（二）系统变更管理 审计人员应关注

组织的应用系统及相关系统基础架构的变更、参数设置变更的授权与审批，变更测试，变更移植到生产环境的流程控制等；（三）系统开发和采购管理 审计人员应关注组织的应用系统及相关系统基础架构的开发和采购的授权审批，系统开发的方法论，开发环境、测试环境、生产环境严格分离情况，系统的测试、审核、移植到生产环境等环节；（四）系统运行管理 审计人员应关注组织的信息技术资产管理、系统容量管理、系统物理环境控制，系统和数据备份及恢复管理，问题管理和系统的日常运行管理等。 第二十二条业务流程层面应用控制是指在业务流程层面为了合理保证应用系统准确、完整、及时完成业务数据的生成、记录、处理、报告等功能而设计、执行的信息技术控制。对业务流程层面应用控制的审计应考虑以下与数据输入、数据处理以及数据输出环节相关的控制活动：（一）授权与批准；（二）系统配置控制；（三）异常情况报告和差错报告；（四）接口/转换控制；（五）一致性核对；（六）职责分离；（七）系统访问权限；（八）系统计算；（九）其他。 第二十三条信息系统审计除上述常规的审计内容外，审计人员还可以根据组织当前面临的特殊风险或需求，设计专项审计以满足审计战略，具体包括但不限于下列领域：（一）信息系统开发实施项目的专项审计；（二）信息系统安全专项审计；（三）信息技术投资专项审计；（四）业务连续性计划的专项审计；（五）外包条件下的专项审计；（六）法律法规、行业规范要求的内部控制的合规性的专项审计；（七）其他专项审计。 第六章信息系统审计的方法 第二十四条审计人员在进行审计与信息技术相关内部控制及流程中可以单独或综合应用下列的审

计方法来获取充分、适当的审计证据以评估信息技术内部控制的设计有效性和执行有效性：（一）询问相关的控制人员；（二）观察特定控制的运用；（三）审阅文件和报告；（四）根据信息系统的特性，进行穿行测试，追踪交易在信息系统中的处理过程；（五）验证系统控制和计算逻辑；（六）登录信息系统进行系统查询；（七）利用计算机辅助审计工具和技术；（八）保证独立性、客观性及职业技能的质量控制前提下，利用其他专业机构的审计结果或组织对信息技术内部控制的自我评估结果；（九）其他 第二十五条信息系统审计人员可以根据需要利用计算机辅助审计工具和技术进行数据的验证、关键系统控制/计算的逻辑的验证、审计样本选取等；审计人员在充分考虑安全的前提下，可以利用可靠的信息安全侦测工具进行渗透性测试等。 第二十六条审计人员在对信息技术内部控制进行评估时，应获得充分、可靠及相关的审计证据以支持审计结论完成审计目标，并应充分考虑系统自动控制的控制效果的一致性及可靠性的特点，在选取审计样本时可根据情况适当减少样本量。在系统未发生变更的情况下，可考虑适当降低审计频率。 第二十七条审计人员在审计过程中进行风险评估，并在此基础上依据信息技术内部控制评估的结果重新评估审计风险，并根据剩余风险来进一步设计审计程序。 第二十八条审计工作底稿应以正式的书面或电子形式进行记录，其中应包含审计程序、审计发现和审计结论以及支持审计结论的审计工作细节及审计证据。审计过程中获取的电子数据应建立严格的电子数据归档措施，并对敏感数据进行严格的保密管理。 第七章审计报告与后续工作 第二十九条在审计实施结束后，审计人员应以充分、

可靠及相关的审计证据为依据形成审计结论与建议，出具审计报告，形成审计结果，追踪审计建议的落实并执行相应后续审计程序。 第三十条当信息系统审计作为综合性内部审计项目的一部分时，审计人员应及时与其它相关内部审计人员沟通信息系统内部审计的发现，并考虑依据审计结果调整其他相关审计的范围、时间及性质。 第八章附则 第三十一条本准则由中国内部审计协会负责解释。 第三十二条本准则自2009年1月1日起施行。 