第2203号内部审计具体准则——信息系统审计

第一章 总 则

第一条 为了规范信息系统审计工作，提高审计质量和效率，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。

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。其他组织或者人员接受委托、聘用，承办或者参与内部审计业务，也应当遵守本准则。

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。

第五条 组织中信息技术管理人员的责任是进行信息系统的开发、运行和维护，以及与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 从事信息系统审计的内部审计人员应当具备必要的信息技术及信息系统审计专业知识、技能和经验。必要时，实施信息系统审计可以利用外部专家服务。

第七条 信息系统审计可以作为独立的审计项目组织实施，也可以作为综合性内部审计项目的组成部分实施。

当信息系统审计作为综合性内部审计项目的一部分时，信息系统审计人员应当及时与其他相关内部审计人员沟通信息系统审计中的发现，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。

第八条 内部审计人员应当采用以风险为基础的审计方法进行信息系统审计，风险评估应当贯穿于信息系统审计的全过程。

第三章 信息系统审计计划

第九条 内部审计人员在实施信息系统审计前，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者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，编制信息系统审计方案。

第十条 编制信息系统审计方案时，除遵循相关内部审计具体准则的规定，还应当考虑下列因素：

（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、外部审计所发现的问题及后续 审计情况；

（七）其他影响信息系统审计的因素。

第十一条 当信息系统审计作为综合性内部审计项目的一部分时，内部审计人员在审计计划阶段还应当考虑项目审计目标及要求。

第四章 信息技术风险评估

第十二条 内部审计人员进行信息系统审计时，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，分析和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。

第十三条 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。

第十四条 内部审计人员在识别和评估组织层面、一般性控制层面的信息技术风险时，需要关注下列内容：

（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。

第十五条 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，内部审计人员应当了解业务流程，并关注下列信息技术风险：

（一）数据输入；

（二）数据处理；

（三）数据输出。

第十六条 内部审计人员应当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设计合理性和运行有效性进行测试。

第五章 信息系统审计的内容

第十七条 信息系统审计主要是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查和评价。

第十八条 信息技术内部控制的各个层面均包括人工控制、自动控制和人工、自动相结合的控制形式，内部审计人员应当根据不同的控制

形式采取恰当的审计程序。

第十九条 组织层面信息技术控制，是指董事会或者最高管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。内部审计人员应当考虑下列控制要素中与信息技术相关的内容：

（一）控制环境。内部审计人员应当关注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。内部审计人员应当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。内部审计人员应当关注组织的信息系统架构及其对财务、业务流程的支持度、董事会或者最高管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）内部监督。内部审计人员应当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当考虑下列控制活动：

（一）信息安全管理。内部审计人员应当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。内部审计人员应当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。内部审计人员应当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。内部审计人员应当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。

第二十一条 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当考虑下列与数据输入、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。

第二十二条 信息系统审计除上述常规的审计内容外，内部审计人员还可以根据组织当前面临的特殊风险或者需求，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合规性专项审计；

（七）其他专项审计。

第六章 信息系统审计的方法

第二十三条 内部审计人员在进行信息系统审计时，可以单独或者综合运用下列审计方法获取相关、可靠和充分的审计证据，以评估信息系统内部控制的设计合理性和运行有效性：

（一）询问相关控制人员；

（二）观察特定控制的运用；

（三）审阅文件和报告及计算机文档或者日志；

（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）利用其他专业机构的审计结果或者组织对信息技术内 部控制的自我评估结果；

（九）其他。

第二十四条 信息系统审计人员可以根据实际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/计算的逻辑验证、审计样本选取等；内部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。

第二十五条 内部审计人员在对信息系统内部控制进行评估时，应当获得相关、可靠和充分的审计证据以支持审计结论完成审计目标，并应当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以根据情况适当减少样本量。在系统未发生变更的情况下，可以考虑适当降低审计频率。

第二十六条 内部审计人员在审计过程中应当在风险评估的基础上，依据信息系统内部控制评估的结果重新评估审计风险，并根据剩余风险设计进一步的审计程序。

第七章 附 则

第二十七条 本准则由中国内部审计协会发布并负责解释。

第二十八条 本准则自 2014 年 1 月 1 日起施行。