广东省注册会计师协会

文　　件

粤注协〔2024〕19号

广东省注册会计师协会关于会计师事务所执行审计业务涉及信息系统审计的风险提示函

各会计师事务所:

随着信息技术在企业日常运营各个环节的深入运用，信息技术对企业财务报告的编制效率及正确性影响也越来越大。会计师事务所对高度依赖信息系统的企业进行相关财务报表审计工作时，应加强对信息技术因素可能导致财务报表重大错报风险的重视。为帮助会计师事务所在审计业务中有效防范信息技术带来的执业风险，广东省注册会计师协会专业指导委员会提示如下:

风险提示1：关注会计师事务所信息技术专业胜任能力对信息系统审计工作的影响

执行信息系统审计工作的相关人员，应具备相应的信息技术

技能和知识，包括熟悉信息系统的规划、设计、开发、运维和安全防护等基础知识，掌握数据分析和代码技能。此外，信息系统审计过程中可能使用到各种专业审计工具，如数据分析软件、系统配置检查脚本、安全评估工具等，执行信息系统审计工作的相关人员也应熟练使用。如信息技术的专业胜任能力不足，可能影响项目审计质量。

会计师事务所应加强对信息系统审计人员的专业培训，提高其技能和知识水平，以有效应对潜在的审计风险。会计师事务所还应对信息系统审计方法论及信息技术相关规范要求进行深入研究，制定信息系统审计工作的标准化和规范化流程。会计师事务所还需要考虑相关专业审计工具的获取和使用过程中是否合法合规，包括关注是否具有软件使用许可、是否存在数据泄露及隐藏恶意代码风险等。

风险提示 2：确定针对被审计单位执行信息系统审计的必要性

注册会计师应对企业的财务数据和业务流程进行深入了解，按照风险导向原则制定整体审计计划，综合考虑重要审计领域及科目所涉及的业务流程及内部控制是否高度依赖信息系统的数据输入和处理、系统自动计算并由系统产出报表，审计工作是否存在无法通过大量的实质性测试工作覆盖所有业务场景以提供合理保证等情况，在项目组内部充分讨论后确定执行相关信息系统审计的必要性。

执行信息系统审计时，除制定常规的信息系统审计程序外，信息系统审计团队需要对复杂的高风险系统给予特别关注。一般情况下，信息系统是否复杂取决于系统类型和数据处理程度，复杂且高风险系统一般包含以下特点：

（一）有复杂的自动化计算逻辑，且对财报数据存在影响，如保费计算、佣金计算、加权平均估值法核算存货成本、复杂模型的成本计提、账单进行多重定价计算等系统。

（二）供应商不再提供维护服务和功能迭代支持但依然存在较多业务场景变化和功能需求变更。

（三）支持企业核心业务且系统间具有广泛定制接口，如生产企业的ERP系统、互联网企业的业务核心平台等。

（四）处理大量交易。

（五）为大型集团、多业务模式企业等复杂经营实体处理信息且具有复杂的架构。

此外，对于 A 股 IPO 项目，按照相关监管要求，报告期内任意一期通过互联网取得的营业收入占比或毛利占比超过 30%，或核心流程高度依赖信息系统的企业，注册会计师原则上均应对该类企业的信息系统可靠性进行专项核查并发表明确核查意见。

风险提示 3：关注被审计单位信息系统审计范围确定的影响

注册会计师应结合对被审计单位信息技术环境的初步了解，按照审计计划中重要审计领域所依赖的信息系统，确定信息系统的审计范围：一是确定重要的财务报表科目、组成部分及重大披

露；二是确定财务报表审计中的重要业务流程和交易；三是识别相关业务流程和交易的潜在错报风险来源；四是确定所识别风险的相关系统应用控制和数据，如系统实现了哪些自动化控制，系统生成的报表或信息，系统支持哪些自动计算，系统实现的权限管理和职责分离情况，系统之间的自动化接口等。

注册会计师需要从包括信息技术风险影响要素确认、系统依赖点范围、信息技术治理环境控制测试范围、信息技术一般性控制测试范围、信息技术应用控制测试范围、信息技术辅助审计范围等方面确定审计方案中的信息系统审计范围。

风险提示 4：关注具体执行信息系统审计过程的规范性和系统性

对目标信息系统执行审计，主要涉及对被审计单位的信息技术治理环境控制（信息系统控制体系的大背景，决定管理的基调和健康程度）、一般性控制（信息系统风险应对体系的基础和内核，为应用控制体系提供稳健持续有效的保证）、应用控制（直接对业务流程进行有效支撑和保障）进行测试，并按需对业务数据执行全量分析。注册会计师收集相关证据、完成相关底稿，最后形成审计发现，评估其对被审计单位整体信息系统的安全性、完整性、可用性目标所造成的影响，进一步评估其对财务报告所产生的影响。

其中，对于治理环境控制测试和一般性控制测试，主要评估其设计有效性及执行有效性。设计有效性主要关注被审计单位对

信息技术各控制点的相关风险是否进行了有效识别并设计了相应的制度和流程来应对，主要体现在是否建立了有效的制度、规程、指引、授权及权限分离等；执行有效性主要关注被审计单位对该控制点是否按照所制定的制度规程要求在报告期内规范有效执行，并能提供清晰可靠的执行有效性证据。大多数情况下，被审计单位可能未严格按照内部控制规范、相关行业规范制定信息技术内控制度，注册会计师需要关注被审计单位信息技术部门是否按照行业约定俗成的方式对信息系统各方面进行有效管控，确认其执行有效。

（一）执行信息技术治理环境控制测试

注册会计师按照对信息技术环境的初步了解，进一步对信息技术治理环境的设计有效性及执行有效性进行控制测试，主要涉及的控制点如下：

1. 治理环境-信息系统组织架构；

2. 治理环境-岗位职责及其分离；

3. 治理环境-信息系统战略规划；

4. 治理环境-信息技术人员招聘与签约；

5. 治理环境-信息技术人员培训与评价；

6. 治理环境-信息技术人员工作变更与终止；

7. 治理环境-信息系统风险识别、评估及响应；

8. 治理环境-第三方管理；

9. 治理环境-信息系统制度体系。

（二）执行信息技术一般性控制测试

信息系统一般控制由四大领域组成：系统开发、系统安全运维、系统变更、程序及数据的访问控制，共同构建了信息技术风险应对体系的内核。

1.针对系统开发控制按照如下各控制点测试系统开发内控设计有效性及执行有效性：

（1）应用系统开发-立项及需求分析；

（2）应用系统开发-详细功能设计；

（3）应用系统开发-编码开发规范管理；

（4）应用系统开发-系统上线前及更新测试；

（5）应用系统开发-数据迁移；

（6）应用系统开发-系统上线；

（7）应用系统开发-系统开发的变更管理。

2.针对系统安全运维控制按照如下各控制点测试系统安全运维内控设计的有效性及执行有效性：

（1）安全运维-物理环境安全；

（2）安全运维-系统环境安全；

（3）安全运维-作业调度；

（4）安全运维-数据备份；

（5）安全运维-备份数据恢复性测试；

（6）安全运维-事件/问题管理；

（7）安全运维-信息系统持续性计划；

（8）安全运维-生产环境与开发测试环境分离;

（9）安全运维-生产环境变更。

3.针对程序和数据访问控制,按照如下各控制点测试系统访问控制内控设计的有效性及执行有效性:

（1）程序及数据访问-物理环境访问控制;

（2）程序及数据访问-超级用户/特权用户;

（3）程序及数据访问-用户账号及身份验证;

（4）程序及数据访问-访问管理/授权审批;

（5）程序及数据访问-用户权限定期审阅。

注册会计师应按照审计准则要求并结合被审计单位实际情况，对各控制点的设计有效性及执行有效性获取常规证据清单，并执行有效性评价，编制治理环境及一般性控制的底稿。

（三）执行信息技术应用控制测试

信息系统应用控制范围的确定是一个由浅入深的过程,在审计的初步规划阶段，注册会计师仅获取应用控制的初步范围，详细审计范围的确定需要在详细审计规划阶段和审计执行初期,通过资深项目负责人对各业务流程进行端到端的了解后才能确定。

通俗地理解，在对被审计单位执行内部控制测试时，应针对选定的重点审计事项所涉及的信息系统(包括业务系统及财务系统)，紧密结合信息系统的控制，通过对不同业务类型选定一个样本执行穿行测试，充分理解流程的发起、流转、审批、处理等业务流程，以及该流程各环节在信息系统中的数据逻辑，需结合

数据流转流程进行跟踪穿行，针对流程数据，验证在每个关键控制点的数据流转的一致性、发起及审批权限的设计合理性及授权匹配性、对数据加工运算的正确性、异构系统接口对数据传输和接收的完整性，以及最后财务核算所依赖报表的输出正确性等。

通过样本穿行，确认系统对数据处理的正确性，并充分识别关键控制点，执行进一步的自动计算/控制测试、报表输出测试、权限测试、接口测试等，如部分自动计算、报表统计生成较为复杂，需要引入信息技术专家对业务逻辑进行复盘（审核代码或者重写处理逻辑对源数据进行运算，比对输出后的数据与系统数据的差异性），并结合 CAATs 分析应对系统日志进行全量数据分析，确认权限控制及数据传输校验的有效性及数据处理逻辑的正确性等审计目标。

整体来说，应用控制应由审计项目组按照对被审计单位的业务流程，结合重点审计事项，对该事项流程所涉及的信息系统按照不同业务类型进行穿行测试，形成穿行测试证据，并规整编制穿行底稿。确认数据流转和加工处理是否正常，进一步确认是否在部分关键控制环节引入信息技术专家辅助执行全量数据测试，确保系统应用控制的有效性。

（四）执行信息技术辅助审计（CAATs）

随着企业的业务流程高度集成于信息化环境中，传统审计程序已无法适应新时代的审计环境及审计需求，基于企业的所有关键交易信息均存储于信息系统中，在被审计单位规模不断扩大，

伴随着交易数据成量级增长的情况下，审计人员很难再依赖人工抽样等传统审计方式对如此大量的数据进行审计。CAATs 相关工具能快速实现海量重复计算，通过数据异常来体现潜在的内控缺陷、反映高风险交易等。在审计程序的实质性测试中，可协助项目组执行系统数据提取、系统数据核对（系统间业务数据一致性核对、业财数据一致性核对）、日记账分析、核心业务数据分析等。

一般而言，执行 CAATs 工作需要经历如下步骤：

1.确立审计范围、目标及关注点；

2.了解审计范围所涉及的数据源系统逻辑和数据库表结构、数据字典、元数据等相关信息；

3.在确保数据源提取准确性的前提下，执行源数据提取并导入 CAATs 分析工具；

4.对导入源数据执行清洗和缺失性分析；

5.基于审计目标及关注点，构建数据分析模型，利用源数据生成模型结果统计数据；

6.对结果数据进行分析，查找异常点，与企业沟通查找原因；

7.形成底稿记录及审计小结。

针对大量的业务数据，信息技术人员可通过如 Excel、PowerBI、Python、ACL、数据库软件等专业工具对数据进行处理和分析，必要时需要有编程能力应对复杂数据处理和结果呈现。

风险提示 5：信息系统审计发现的影响评估和追加审计程序

的充分性

需要注意的是，信息系统审计和财务报表审计应服务于同一个审计目标，作为一个审计整体互相配合，不能将信息系统审计从财务报表审计中割裂出来作为一个低耦合的工作模块。特别是当信息系统审计团队识别到信息系统存在控制缺陷或数据存在不一致或违反逻辑等异常情形，需要及时有效地与财务报表审计团队或团队内其他审计小组就信息系统相关问题进行沟通，评估该缺陷及数据异常对于现有审计程序的影响，以及是否需要额外采取适当的追加审计程序，如增加对于手工补偿性控制的测试、调整实质性测试程序的样本数量等。该评估过程以及评估结论需要在相关的工作底稿中进行恰当记录。

信息系统审计是一项专业性强的综合性工作，涉及多个领域，要求会计师事务所从业人员具备较高的专业胜任能力。为了更好地开展审计工作，从业人员需要熟悉信息技术基本理论及各类软件技术，同时结合被审计单位的信息系统进行审计。在财务报表审计中，注册会计师需要对财务报表是否在所有重大方面按照适用的财务报告编制发表审计意见。审计准则要求注册会计师应当了解与审计有关的内部控制、了解与财务报告相关的信息系统、了解企业如何应对信息技术导致的风险并确定审计应对。因此，不管是否执行信息系统审计程序，注册会计师都需要对被审计单位的信息系统整体环境进行了解，按照被审单位对信息系统的依赖程度和系统的复杂性程度确定执行信息系统审计的范围。

本提示函仅供注册会计师在执业过程中参考，并未涵盖会计师事务所执行审计业务涉及信息系统审计的全部关注事项以及可能面临的全部风险，也不能替代相关法律法规、执业准则以及注册会计师的职业判断。会计师事务所及其从业人员在执业中仍需结合项目实际情况以及注册会计师的职业判断开展工作。

广东省注册会计师协会

2024 年 1 月 15 日

公开方式：主动公开

抄送：各地级以上市注协

省注协综合部　　2024 年 1 月 15 日印发