北京注册会计师协会专业技术委员会
专家提示——审计工作底稿的电子化及对第三方电子函证平台安全可靠性的评价

本专家提示仅供会计师事务所（简称事务所）及相关从业人员在执业时参考，不能替代相关法律法规、注册会计师执业准则以及注册会计师职业判断。事务所及相关从业人员在执业中需结合项目实际情况以及注册会计师的职业判断确定，不能直接照搬照抄。

审计工作电子化是会计师事务所提高审计效率、强化质量管理、适应现代信息技术发展的重要变革。审计工作电子化对审计工作底稿的影响是全面的，不仅改变了审计底稿的编制、存储和使用方式，还对审计人员的胜任能力、事务所的审计流程和质量风险管理提出了新的要求。

在审计工作电子化进程下，审计工作底稿的完整性、安全性、一致性及电子底稿的借阅管理在事务所质量管理过程中被高度关注。审计准则对审计工作底稿的格式、内容、范围以及归档作出了具体规定；国家网络信息安全相关法律法规，包括财政部、国家互联网信息办公室于 2024 年 4 月 15 日发布的《会计师事务所数据安全管理暂行办法》（财会〔2024〕6 号）对事务所审计工作中数据处理活动的安全性予以了规范，事务所的审计工作需要满足上述合规要求。《中

国注册会计师审计准则问题解答第 2 号——函证》（2019 年 12 月修订）对注册会计师利用第三方函证平台实施函证程序作出相关规定，要求注册会计师对第三方平台的安全可靠性（如第三方函证平台如何保证函证相关方身份的真实性、信息传输安全性以及记录函证控制过程的完整性等）进行评价，以防范相关审计风险。

北京注册会计师协会专业技术委员会对北京地区会计师事务所审计底稿电子化情况以及第三方电子函证平台使用情况开展了问卷调查，并邀请有关事务所、第三方电子函证平台、行业管理部门专家等进行了专题研讨。在本提示编写过程中，参考了上述调研、研讨的相关资料。

一、关于审计工作底稿的电子化

（一）审计工作底稿的完整性

1.审计工作信息化推动了底稿的电子化

根据《中国注册会计师审计准则第 1131 号——审计工作底稿》，审计工作底稿是注册会计师对制定的审计计划、实施的审计程序、获取的相关审计证据以及得出的审计结论的记录。审计档案，是指一个或多个文件夹或其他存储介质，以实物或电子形式存储构成某项具体业务的审计工作底稿的记录。审计证据是为了得出审计结论和形成审计意见而使用的信息，包括构成财务报表基础的会计记录所含有的信息以及从其他来源获取的信息。审计过程中获取的审计证据，有以电子形式获取的，也有以纸质形式获取的；有从被审计单位内部获取的，也有从被审计单位外部获取的。

审计实务中，由线下审计为主的传统模式正在逐渐转变为基于云技术的审计作业平台等为主的在线审计模式。传统模式下的审计工作底稿主要是以纸质形式为主存档，项目组对审计过程中编制或取得电子形式底稿（如审定表、明细表等）打印后以纸质形式进行归档存储。在线审计模式下，审计工作底稿主要是以电子形式为主存档，如将获取外部证据（如函证回函、重要合同等）进行扫描并插入审计作业软件中。

除审计作业软件外，事务所目前可能还运用函证系统、独立性系统及监盘系统等各种辅助审计工具，函证底稿、独立性底稿及监盘底稿等会分散在不同的审计工具中。如何将分散在不同系统或工具中的底稿统一、及时、完整归档是事务所审计底稿电子化要解决的主要问题。项目组在对不同作业系统（工具）形成的审计工作底稿和留存的审计证据进行统一集中归档时，应当确认审计底稿信息及审计证据内容完整、与相关作业系统（工具）或纸质底稿的一致性，可以通过建立电子档案目录等形式进行电子档案的归集，以便于查阅和管理。

2.纸质形式审计证据归档的完整性

当事务所采用电子方式归档时，电子底稿是主体，审计中获取的电子证据、纸质证据需要在电子底稿中进行索引。审计获取的重要的纸质证据需要立卷归档，事务所如因审计业务涉及民事赔偿诉讼、外部检查，可能会被要求提供这些纸质证据以支持审计工作中形成的相关审计结论和审计意

见。审计人员需要保证归档的电子底稿和纸质底稿的完整性，以证明注册会计师已按照审计准则和相关法律法规的规定计划和执行审计工作。

前述重要的纸质证据主要包括被审计单位或其他相关方签章的业务约定书、管理层声明书、未审财务报表和经审计的财务报表、询证函回函等，还可能包括涉及重大错报风险领域和关键审计事项的应对程序、审计调整、内控缺陷、影响审计意见类型和报告内容要素，或者与疑难事项、意见分歧相关的合同等文件，以及项目合伙人认为重要的其他纸质审计证据。

实务中，对于是否将纸质证据扫描并同时进行电子归档，不同事务所内部质量管理制度可能有不同的规定，有的事务所要求将纸质证据扫描件进行电子归档，有的不作该要求，二者各有利弊。前者，便于快速检索和调用，而且整套电子档案可以通过备份、加密等方式得到保护，即使纸质文档出现问题，完整的电子档案仍能一定程度上为审计结论提供支撑，不足在于扫描存储需要投入相应时间和成本，以及需要考虑扫描件的法律证明力。后者，不需要投入资源进行纸质证据的电子化处理，但纸质文件的检索和查阅通常比电子文件更耗时。事务所在确定其具体做法时，需要对相关成本效益进行综合评价。

审计人员在审计过程中检查被审计单位的相关文件资料，如果认为有必要将该相关文件的副本作为审计工作底稿，直接拍照或将其扫描件作为审计证据可能存在一定的风险。

比如，被审计单位可能否认其存在与事务所电子审计档案中的某一扫描件相对应的纸质原件。项目组根据对项目审计风险的评估情况，可能采取不同的做法。对于重要的审计证据，审计人员应核对取得的复印件与原件相符，并尽可能要求被审计单位在复印件上盖章，以证明是由被审计单位提供。

3.项目质量复核记录的归档

按照事务所质量管理准则以及事务所内部政策，有的项目需要执行项目质量复核，项目质量复核人员就项目质量复核形成工作底稿，以使未曾接触该项目的、有经验的执业人员了解项目质量复核人员（包括协助人员）所执行程序的性质、时间安排和范围。项目质量复核底稿（包括质量复核程序的记录、复核人员与项目组的沟通记录、复核发现的重大问题及项目组的答复等）非常重要，是事务所遵守质量管理准则规范执业的体现，也是事务所内、外部检查中关注的重点，应包含在审计项目工作底稿中。

《中国注册会计师审计准则第 1131 号——审计工作底稿》应用指南中指出，审计工作底稿不需要包括已被取代的审计工作底稿的草稿或财务报表的草稿、反映不全面或初步思考的记录、存在印刷错误或其他错误而作废的文本，以及重复的文件记录。项目质量复核人员在复核过程中可能就某一事项与项目组进行多次沟通，当项目质量复核通过审计作业软件中的项目质量复核模块进行的情况下，在对项目质量复核底稿进行归档时，也应考虑该准则这一方面的要求，避免因存在中间稿而导致对项目质量复核工作不必要的歧义。

4.电子审计档案的存储方式

事务所应根据其实际情况确定电子底稿的存储方式。目前本地存储仍是主流，比如事务所服务器集中存储、光盘或移动硬盘存储。无论采取何种方式保存电子工作底稿，事务所均需要建立并维护与工作底稿相关的政策和程序，以确保不存在任何人未经授权、批准并在有效监控情形下接触已归档的工作底稿。

随着审计程序执行方式的变化，视频监盘、视频访谈、电话访谈及借助智能化工具的资金流水核查等信息化方式普遍应用，审计证据除常见的 Word、Excel 电子文档外，通常还包括图片、照片、音频、视频等多媒体资料。对于审计中获取多媒体形式的审计证据，有的事务所是将其上传到审计作业系统中，与其他电子底稿一并归档存储；有的则是将这些多媒体证据单独存储。在确定多媒体证据的存储方式时，事务所需要对多媒体资料的具体格式作出统一规定，并综合考虑成本、数据容量、网络环境等因素，避免事务所的网络带宽和服务器可能无法承载。如前所述，无论以何种方式存储，项目组均需根据档案目录确认底稿内容完整、索引正确。

5.出具审计报告后或审计档案归档后对电子审计工作底稿的修改

《中国注册会计师审计准则第 1131 号——审计工作底稿》对报告出具后以及底稿整理归档后审计工作底稿的修改，均作出了规定：（1）在某些例外情况下，如果在审计报告日后实施了新的或追加的审计程序，或者得出新的结论，应当

记录遇到的例外情况，实施的新的或者追加的程序、获取的证据和得出的结论，对审计报告的影响，以及对底稿作出相应变动的时间和人员，复核的时间和人员；(2)档案归档后，如发现有必要修改或新增审计工作底稿，无论修改或增加的性质如何，均应记录理由、时间和人员，以及复核的时间和人员。

《会计师事务所数据安全管理暂行办法》规定，会计师事务所应当对审计业务相关的信息系统、数据库、网络设备、网络安全设备等设置并启用访问日志记录功能。 涉及核心数据的，相关日志留存时间不少于三年。涉及重要数据的，相关日志留存时间不少于一年；涉及向他人提供、委托处理、共同处理重要数据的相关日志留存时间不少于三年。

因此，审计报告出具后或底稿归档后，对电子底稿的修改或新增要遵守审计准则以及数据安全管理办法对日志留存时间的规定。

鉴于电子底稿具体修改内容可能难以追踪，或者对个别工作底稿的修改或新增会导致工作底稿整体显示的归档日期有所改变，从而无法支持审计项目组已在规定时间内归档这一事实，因此，如果在审计工作底稿归档之后需要对电子底稿做出修改或新增时，建议另外编制电子底稿，并明确说明修改或新增的原因和范围，而非在原电子底稿中直接进行修改。目前对电子底稿的修改或新增，较为常见的是针对监控活动或外部检查发现的项目审计问题所作整改，如果整改内容无法在该项目当年工作底稿中反映，而是需要在以后年

度审计中进行，项目组可以将相应的整改措施及落实情况记录于后续年度审计底稿中。

对审计档案的任何修改或增加都必须有明确审批和复核记录，以证明不是对审计底稿的伪造、篡改或损毁，不存在这方面的嫌疑，比如，因事务所监控活动需要对底稿进行整改的，依据的是事务所内部监控整改报告；如果是外部检查要求整改，则依据外部检查意见或是监管函或处罚决定书等。事务所需要制定审计档案修改相关内部审批流程，确保对电子审计档案的任何修改均经过适当审批。

（二）审计工作底稿的一致性

1.不同审计作业系统之间数据传输的一致性

当事务所存在多种审计工具，比如审计作业软件、函证系统、独立性系统等，审计工作底稿信息在不同系统之间自动传输、归集时，需要关注和测试数据传输是否完整、一致，避免相关应用系统的设计或内部控制存在缺陷而出现系统性风险。

2.纸质底稿扫描件与原件的一致性

如果事务所内部质量管理制度要求将纸质底稿进行扫描并在电子档案中归集，事务所需要采取一定措施，确保扫描件与纸质底稿一致。比如，规定扫描流程，对扫描件是否清晰、无缺页遗漏等进行检查。当审计过程中纸质底稿更新时，应确保扫描件随之更新。

3.审计软件中导出的归档底稿与软件中底稿数据的一致性

审计软件环境下所查阅的底稿依赖软件数据库的链接支持，从审计软件中导出用于归档的底稿时，需要形成不依赖审计软件即可查阅的档案，要确保审计软件设计正确，归档底稿与审计软件环境下所见底稿一致，内容完整。导出的归档底稿应设置为不可更改模式。

（三）审计工作底稿的安全性

1.监管部门对审计工作电子化安全性的指导

在《会计师事务所数据安全管理暂行办法》中，就事务所如何贯彻落实国家网络数据安全规定予以了细化指导，要求规范数据的分类分级和底稿管理，强调网络管理安全可控，其中对底稿存储地、数据备份、系统权限设置、底稿出境审批等均作出了规定：

（1）审计工作底稿应当按照法律、行政法规和国家有关规定存储在境内，相关加密设备应当设置在境内并由境内团队负责运行维护，密钥应当存储在境内。

（2）应当建立数据备份制度，确保在审计相关应用系统因外部技术原因被停止使用、被限制使用等情况下，仍能访问、调取、使用相关审计工作底稿。

（3）应当拥有审计业务系统中网络设备、网络安全设备的自主管理权限，统一设置、维护系统管理员账户和工作人员账户，不得设置不受限制、不受监控的超级账户，不得将管理员账号交由第三方运维机构管理使用。加入国际网络的事务所使用所在国际网络的信息系统的，应当采取必要措施，使其符合国家数据安全法律、行政法规和该暂行办法的规定，

确保事务所的数据安全。

（4）对于审计工作底稿出境事项，事务所应当建立逐级复核机制，采取必要措施严格落实数据安全管控责任。对于需要出境的审计工作底稿，按照国家有关规定办理审批手续。

该暂行办法中还就事务所对核心数据的四级网络安全等级保护、重要数据的三级及以上网络安全等级保护，以及数据汇聚、关联后属于国家秘密事项的安全保护等作出了要求。

该暂行管理办法2024年10月1日起施行，事务所在设计和执行电子底稿安全性相关政策及程序时，必须符合该暂行办法的相关规定。

2.审计工作底稿电子化过程中对网络安全的考虑

事务所应建立完善的网络安全管理治理架构，建立健全的内部网络安全管理制度体系，包括内部决策、管理、执行和监督机制，提高网络安全管理能力，为审计工作底稿电子化提供安全的网络环境。事务所使用网络版审计软件进行审计作业，或者采用服务器、云平台存储电子审计工作底稿时，需要对关键的网络安全事项予以关注，提高审计工作的网络安全性，比如：

（1）数据保护及访问控制：确保审计过程中收集分析数据是安全的，实施严格的访问控制措施，确保只有经授权的审计人员能够访问审计数据系统，防止未经授权的访问和泄露。

（2）数据完整性：使用加密和其他技术来保护数据不被

篡改，确保审计证据的完整性。

（3）网络安全策略：制定和执行网络安全策略，包括防火墙、入侵检测等，确保电子审计底稿在规定的审计工作保存期限内安全存储。

（4）风险评估：定期进行风险评估，以识别和评估可能影响审计过程的网络安全威胁。

（5）应急响应计划：制定应急响应计划，以在发生安全事件时迅速采取行动，减少潜在损害。

（6）员工培训：对审计团队进行网络安全意识培训，确保了解潜在的风险和最佳实践。

（7）技术更新：随着技术的发展，定期更新审计工具，以应对新的网络安全威胁。

3.防范电子审计底稿未经授权扩散可能导致的风险

事务所对审计底稿中的被审计单位信息负有保密义务。因日常监管需要，事务所需要向监管机构提供电子审计底稿，或者开放审计作业软件。为了防范底稿内容未经授权扩散可能带来的风险，事务所需要采取相应的保密措施。比如，有的可能使用具有外发文件控制功能的数据安全产品，对外发文件设置查阅期限、密码验证、修改限制、打印限制、过期自毁等操作权限，确保资料能够共享查阅，并防范越权读取或二次扩散，以保护底稿及所载客户信息的安全。

4.接受境外监管时工作底稿的提供

事务所接受境外监管需要向境外监管机构提供审计工作底稿时，通过监管合作渠道提供。事务所需要调出包含电

子底稿在内的整套审计档案，对涉密敏感信息（包括国家机密、商业秘密和个人隐私数据等）进行筛查，聘请律师对保密合规性出具法律意见书；可能还需要依据有关监管法规的要求，将底稿、法律意见书提交相关政府管理部门，对底稿保密合规性作进一步审查。事务所向相关档案管理部门申报底稿出境事项，审批通过后，由相关政府管理部门将工作底稿转交境外监管机构。

（四）电子审计工作底稿借阅管理

实务中，在审计数字化和严监管形势下，电子审计工作底稿可能会被大量借阅。一方面外部检查可能强制要求提供电子版；另一方面主要是由于内部需求借阅，比如内部监控需要调阅，或项目组因 IPO 申报加期审计、IPO 反馈问询回复等需要查阅前期底稿，年报审计需要查阅上年工作底稿等。为保证归档后电子审计工作底稿的完整性、安全性及一致性，事务所有必要加强对电子审计工作底稿的借阅管理。

（1）对借阅权限、借阅方式等作出相关规定。对电子工作底稿借阅必须履行事务所内部借阅审批程序，对借阅权限进行规定，如仅能在线查看、支持在线查看和打印、规定在线查看时间等。

（2）电子底稿归档后应以权限管理为基础，支持多途径、多角度且易用的检索和利用方式，满足用户各类查档需求。支持用户在审批权限许可范围内在线查看、打印目录数据或电子底稿文件时，如有必要，应限制用户对电子底稿的具体文件、具体页面的可阅读范围，对电子底稿的下载履行内部

审批、添加数字水印和授权阅读时间等。

二、关于第三方电子函证平台安全可靠性的评价

1.对第三方电子函证平台安全可靠性评价的总体要求

通过独立、安全可靠的第三方电子函证平台进行函证，既能提高函证程序执行效率，又能有效应对传统纸质函证过程中可能存在的舞弊风险、提升函证程序执行质量。实务中，第三方电子函证平台（也称“第三方电子询证函平台”）主要包括两类：一类是专门提供函证服务的第三方平台（如中国银行业协会银行函证区块链服务平台、境外的confirmation.com），另一类是被询证者自身的电子函证平台（如工商银行函证e信）。

《<中国注册会计师审计准则第 1312 号——函证>应用指南》（2023 版）第 13 段要求，如果被询证者利用第三方协调和提供回函，注册会计师可以实施审计程序以应对下列风险：（1）回函来源不合适；（2）回函者未经授权；（3）信息传输的安全性遭到破坏。《监管规则适用指引-审计类第 2 号》指出事务所存在利用第三方函证平台执行函证程序时未了解平台的资质或安全性、可靠性情况、未能保持职业怀疑的问题。

值得说明的是，根据《中国注册会计师审计准则问题解答第 2 号——函证》规定，商业银行等金融机构自身的电子函证平台，由于商业银行等金融机构负责按照相关法律法规建立和完善有关回函的内部控制，并依法对其出具的回函承担相应的法律责任。一般而言，除非出现相反情况，注册会

计师无需对商业银行等金融机构自身的电子函证平台内部处理过程的安全可靠性进行专门评价。

对第三方电子函证平台的独立性、安全可靠性评价工作在行业协会层面或事务所层面统一完成更符合成本效益原则。项目组在应用金融机构自身的电子函证平台外的其他第三方电子函证平台进行函证时，如果没有行业协会或事务所层面对第三方电子函证平台安全可靠性的评价，项目组需要遵照准则要求实施相关评价工作。

另外，根据《中国注册会计师审计准则第 1241 号——对被审计单位使用服务机构的考虑》规定，如果拟利用服务机构（即本文的第三方电子函证平台，下同）注册会计师出具的第一类报告（即针对服务机构对控制的描述和设计出具的报告）或第二类报告（即针对服务机构对控制的描述、设计和运行有效性出具的报告）作为审计证据，以支持对服务机构内部控制设计和执行情况的了解，注册会计师应当：（一）评价对服务机构控制的描述和设计所针对的时点或期间是否适用于注册会计师的审计目的；（二）对了解与审计相关的服务机构内部控制而言，评价报告提供的证据是否充分和适当；（三）确定服务机构系统描述中明确的被审计单位的互补性控制是否与被审计单位相关；如果相关，了解被审计单位是否设计和执行了此类控制。

如果注册会计师在评估重大错报风险时预期服务机构的控制的运行是有效的，注册会计师应当实施下列一项或多项程序，以获取有关这些控制运行有效性的审计证据：（一）

获取第二类报告（如可行）;（二）对服务机构的控制实施适当测试;（三）利用其他注册会计师代其对服务机构的控制实施测试。

2.对第三方电子函证平台安全可靠性的评价要点

事务所层面应建立应用第三方电子函证平台进行函证的审计政策和程序，明确对第三方电子函证平台独立性、安全可靠性的评价内容要求和评价周期。第三方电子函证平台通常会聘请具有胜任能力的注册会计师（或信息安全认证机构等）对第三方电子函证平台的内部控制有效性出具鉴证报告。

事务所应当判断是否利用第三方电子函证平台注册会计师出具的内部控制有效性鉴证报告来评估其安全性可靠性，并对评价结果定期更新。如事务所不能利用该报告，则应当对第三方电子函证平台进行直接测试。

如事务所利用内部控制有效性鉴证报告对第三方电子函证平台进行安全性可靠性评估，则需要执行以下程序：

（1）获取第三方电子函证平台注册会计师出具的内部控制有效性鉴证报告及相关资料;

（2）对以下内容进行了解和记录：

①鉴证工作执行的依据、报告结论以及适用范围;

②鉴证工作涵盖的期间及时间间隔;

③鉴证工作的测试范围、测试过程、取得的证据及测试的结果（包括互补性控制是否相关且有效）;

（3）评估内部控制有效性鉴证报告中列示的工作是否

支持形成第三方电子函证平台进行安全可靠的结论，判断是否需要执行额外的测试程序；

（4）评估第三方电子函证平台聘请的信息安全认证机构或专业人员的胜任能力、专业素质和独立性；

（5）了解平台及其所有者和运营商的组织架构，关注其是否存在被监管机构处罚、涉诉等信息，了解鉴证报告出具日期至评估工作完成日期之间平台控制环境的变化情况等。

一般情况下，对第三方电子函证平台的安全认证应当至少每年获取一次最新的鉴证报告，并在开展审计工作之前获取。如果最近一次出具的鉴证报告的日期与审计外勤日间隔较长，导致对第三方电子函证平台的安全性评价所依据信息或情况已发生重大变化，注册会计师应评价对审计工作的影响程度。

3.正确看待在银行函证平台中发出的某些询证请求未能通过银行参数校验问题

在相关各方共同努力、有序推进下，内地银行函证工作已经可以通过银行函证电子平台进行，比如中国银行业协会银行函证电子平台、中国互联网金融协会银行函证电子平台、中国金融认证中心银行函证电子平台，事务所根据需要自行申请接入使用。

通过银行函证平台发函时，如果询证请求中的某些参数不符合相关银行的校验规则时，询证请求无法通过，发函失败可能降低收发函效率。事务所需要重视该问题，采取应对措施：

一是正确看待问题。对询证请求进行校验，是银行业金融机构推进银行函证电子化所采取的安全措施。相比于审计人员采用纸质函证在发函回函控制中所投入的时间精力、对函证过程相关信息的审核以及等待回函所需的时间，使用银行函证平台的效率是明显的。事务所内部需要就此确定相应的政策和程序，作出相关规定和要求。

二是事务所负责银行函证集约化处理的部门或人员，需要及时汇集审计人员在使用银行函证平台中可能遇到的、提出的各种问题，第一时间向银行函证平台反馈，请求协调解决，并将确认的问题成因、解决办法、注意事项及时在全所通报，信息共享。

总审：邱连强、宋振玲

执笔：张革、蒋玉芳

意见反馈：杨绯、刘虓、王晓瑞、都蕾
何先琴、韩天佩、胡方勇

校对：万思宁