DOI:10.19641/j.cnki.42-1290/f.2018.15.025

云审计系统构建及其风险控制

罗 婧[1]，王 炜[2]

【摘要】云审计作为审计技术的优化创新迎合了大数据时代的审计新需求。通过对云计算的分析，认为云审计服务可按照云计算服务框架分为IAAS、PAAS和SAAS。在云计算IAAS、PAAS和SAAS 等服务模式的基础上，首先从被审计端、云端和审计终端三个视角构建云审计应用系统，然后具体分析其在实际应用中可能存在的潜在风险。最后，从被审计端风险控制、云端风险控制、审计终端风险控制三个方面提出针对性的建议。

【关键词】云审计；云计算；云审计系统；风险分析；风险控制

【中图分类号】F239.1　　【文献标识码】A　　【文章编号】1004-0994(2018)15-0144-6

一、引言

“十三五”审计规划明确指出各级审计机关应不断优化审计技术和方法，提高审计效率，满足审计全覆盖内在要求。但是大数据时代产生的海量数据使得传统审计技术难以满足监督需求，革新审计技术势在必行。而云计算依靠虚拟化、分布式存储等关键技术，实现了海量数据的采集、存储、分析及报告等，有效迎合了大数据时代的审计新需求。利用云端提供的不同层次服务，审计终端和被审计端可以摆脱自建硬件设备和自行开发审计应用软件的成本支出，借力云端的智能化数据处理、分析功能，提高审计效率。同时，云审计能够摆脱传统审计技术强调的数据传输、转换、汇总等繁杂程序并解决不同审计软件兼容性问题，使审计人员聚焦于审计任务本身。可见，云审计的广泛应用不仅节约了审计成本，还能提高审计效率并保证审计质量。

但是相较于传统审计技术，云审计系统运作的复杂性也导致其背后隐藏的风险和危害远高于传统审计技术，如何有效应对新环境下云审计应用可能产生的风险，将成为大数据时代云审计能否广泛应用的关键。因此，本文从被审计端、云端和审计终端三个视角出发构建云审计应用系统，并分析其在具体应用中可能存在的风险，进而提出针对性的建议，以期为未来审计机关在大规模应用云审计应对可能发生的风险时提供借鉴和参考。

二、云计算与云审计概述

(一)云计算

云计算是在大数据时代背景下产生的一种全新的领先信息技术，其依靠虚拟化、大规模数据处理及分布式存储等核心技术，实现了海量数据的实时采集上传、加工汇总、分析及存储等，有效摆脱了本地和远程计算机的限制，为用户解决了数据中心管理、海量数据存储空间、大规模数据处理分析以及应用程序更新改造等现实性难题，用户只要按需付费就可随时随地便捷访问和利用云资源，在提高服务质量的同时还能有效降低运行和维护成本。

从用户体验的角度出发，云计算主要提供三种服务模式：基础设施服务(IAAS)、平台及服务(PAAS)、软件及服务(SAAS)。如图1所示，IAAS层是云计算服务框架的基础层，能够为用户提供服务器、防火墙、存储设备和网络设备等基础设施服务，有效减少用户软硬件设备开发成本，最大限度地实现资源共享和数据存储[1]。PAAS层是云计算服务框架的平台层，主要为用户提供集应用程序设计、开发、测试、部署与托管为一体的完整系统应用平台，解决用户自建系统应用平台的内在需求。SAAS层是

云计算服务框架的应用层，为用户提供应用程序等软件服务，用户不需自行安装软件产品而是直接使用云端提供的软件服务，有效降低了用户的日常维护成本。

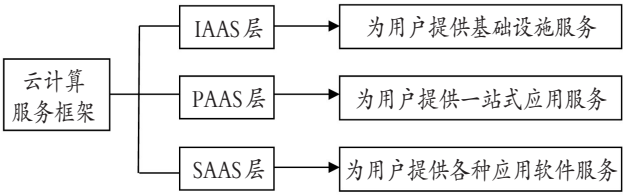

图 1 云计算服务框架

（二）云审计

云审计是云计算技术与审计工作相结合的技术创新产物，即利用“云端”提供的云计算服务平台，归集和管理审计所需的各类资料和数据，对容纳的数据进行实时更新和有机集合，能够智能控制对审计模型的选择和使用，从而实现审计信息的数字化与智能化处理，促进信息共享和沟通，保证审计质量。随着大数据时代的到来，云审计能够依靠虚拟化、可动态扩展、大规模分布式计算模式等关键技术，将网络上闲置存储设备、计算能力、应用软件等资源集中起来[2]，为审计主体提供包括数据采集、加工、汇总、分析和存储等多元化、智能化、数字化的数据服务，降低审计主体对自建软硬件设备的依赖，实现低成本高效率的审计作业服务。

按照云计算服务框架，也可将云审计分为IAAS、PAAS和SAAS三个层次。其中：IAAS层主要通过租用基础设备，使用云端提供的云储存、虚拟计算机等基础功能，降低硬件投入成本；PAAS层是审计软件应用平台，为开发审计软件、审计模型和审计工具提供共享环境；SAAS层主要通过云端web提供软件应用服务，审计主体只需支付资源使用费即可实现审计项目和资源的有效管理，降低自装软件的维护和更新成本。由此可见，云审计的广泛应用能够有效解决审计软硬件设备难题，以及审计数据存储、加工、分析、共享和工作失效等问题，审计人员只需注重于审计任务本身，可最大限度地提高审计工作的效率和科学性。

三、云审计系统构建

考虑到传统审计技术难以适应大数据时代产生的海量数据审计需求，本文借鉴云计算技术的数据存储、分析、加工等优势，在兼顾审计成本、审计效率和数据安全的前提下，将云技术的数据处理优势融入审计实践工作中，通过按需付费直接使用云端提供的SAAS、PAAS、IAAS等服务，对被审计端开展审计作业，可在提高审计效率的同时有效降低审计成本。构建的云审计系统如图2所示。

1. *在被审计端和审计终端融入第三方云计算服务提供商（简称“云端”）。*构建一个由云端作为第三方服务中介、审计终端和被审计端作为用户层的云审计应用系统。其中，被审计端应按期汇总财务收支数据，在此过程中应重点关注原始数据的完整性和真实性，防止人为删减和更替数据，以保证数据源头的完整、准确和真实。同时，按照审计端的审计要求，及时通过云端接口技术将原始财务收支数据上

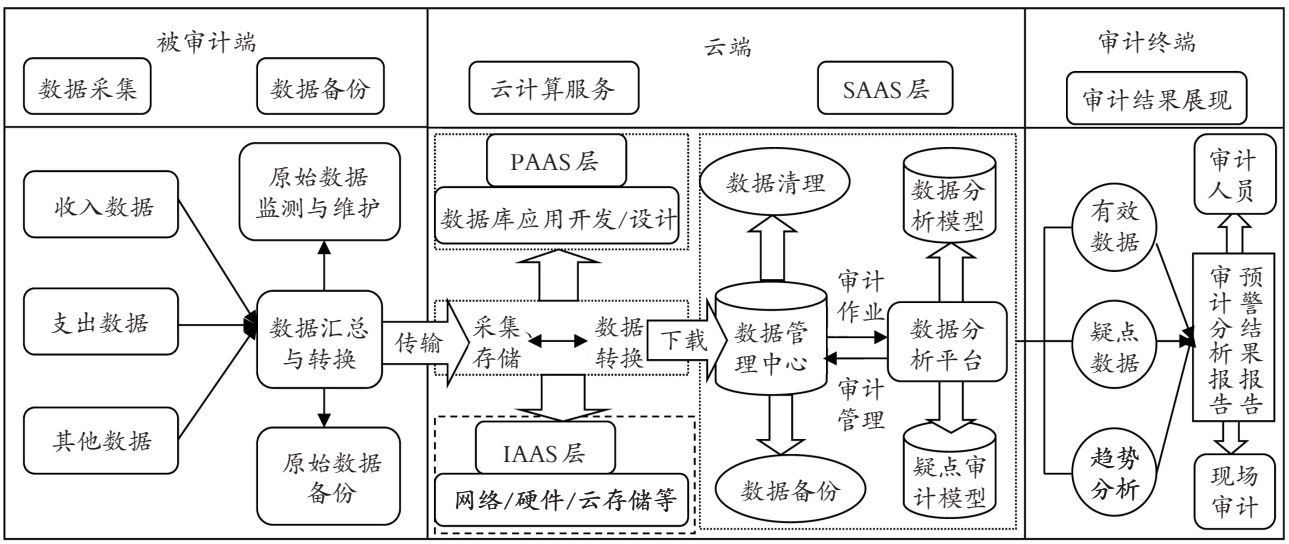

图 2 云审计系统

传至云端，并对传输数据进行备份，防止数据上传失败或上传不完整。

2. 云端根据审计终端需求，为其提供数据采集、数据加工转换、数据分析和存储以及审计分析报告等服务。主要服务内容包括：

（1）利用IAAS层实现海量数据存储。审计数据的爆炸性增长带来了原始数据存储空间不足的难题，传统审计数据大多存储在U盘、硬盘或依靠磁介质传送到指定的数据存储中心，容易造成数据缺失，存在数据安全性不高、共享性差等问题。而云端提供的存储器、网络资源和安全机制等为审计机关存储海量数据提供了有利的硬件条件，再加上虚拟化技术和数据集群能够将不同类型、不同格式的存储资源整合起来以统一的形式实现存储服务，因此审计终端无须单独配置存储器、服务器等硬件设备，只要借助云平台即可实现海量数据存储目标。

（2）利用PAAS层实现数据共享与加工。通过平台层提供的应用开发与设计模块、数据缓存等标准化服务，能够使得开发设计的审计软件具有较好的兼容性和一致性，可以自由切换并实现不同格式数据之间的共享和传输，集成的应用开发环境有效提高了所获数据的有效性和共享性。同时，数据库等服务模块能够将IAAS层存储的数据进行整合加工，并以统一化、标准化的形式传输到后台的数据处理中心，进而有助于提升审计数据处理效率。

（3）利用SAAS层实现数据智能分析及预警。数据管理中心是审计实施系统和审计管理系统交互管理的中转站，作为数据智能分析处理的中心数据库，其依靠综合信息数据库、专家经验数据库和法律法规数据库等，对被审计端上传的数据进行智能化处理，通过数据分析平台自带的分析模型和审计模型，对原始数据进行智能加工以发现可疑数据和审计线索，并自动生成预警报告。

3. 审计终端是审计结果的展现。审计终端无须自建软硬件设备，只需要按期付费就能通过电脑、手机等网络终端直接登录云平台，查看被审计端上传的原始数据，下载云端对原始数据加工转换后的备份数据，调取数据管理中心智能化识别的可疑数据和预警报告，并按照云端数据分析处理结果指导现场审计工作实践。由此可见，借助云计算不仅能够实现审计终端对被审计端的有效审计作业，还能降低不必要的软硬件开发及维护成本；不仅能够提高审计效率，还能有效保障审计质量。

四、云审计系统应用风险分析

（一）被审计端风险分析

被审计端作为财务原始数据采集的源头，应保证上传云端原始数据的真实性和完整性。因为真实、完整、准确的原始数据直接关系到云端数据管理中心对于审计数据分析报告和数据处理结果的科学性和可靠性的影响，进而影响审计终端利用云端审计数据分析报告和预警分析报告指导现场审计的成败。具体而言，被审计端风险主要如下：

第一，当前被审计端数据采集和传输都建立在互联网的基础上，而网络环境的开放性和共享性容易导致被审计端数据采集安全性和稳定性不足的问题，网络病毒和黑客的恶意攻击加剧了被审计端网络安全运行的风险，难以有效保证被审计端原始数据采集的数量和质量。

第二，当前数据都以无纸化的电子数据进行采集和传输，数据存储也主要依靠磁介质，而电子数据的删改无法留下痕迹，这为能够接触到原始数据的舞弊者更改数据提供了契机，舞弊行为的无处可寻增加了被审计端原始数据完整性和准确性的风险。

第三，原始数据的实时采集和连续更新对被审计端网络硬件设施提出了更高的要求，计算机内存不足、系统卡顿或瘫痪、网络传输能力有限等现实性问题都可能影响数据采集端口的连续性和完整性。而系统区与数据区的混合使用也加剧了系统配置风险，导致数据保存和备份面临较大挑战。

第四，在保证原始数据采集完整性和准确性的基础上，被审计端还要依靠网络接口技术将数据传输到云端，在此过程中数据传输安全性和稳定性则依赖于每个基础API（应用程序编程接口）内置的安全性，而数据传输接口端API中的不安全因素可能会导致数据传输失败，甚至是数据外泄[3]。

（二）云端风险分析

云计算利用虚拟化、可动态扩展、分布式数据存储等关键技术，将网络资源集中整合起来，有效释放了被审计端数据存储和硬件设备的内在压力，也为审计终端提供数据加工、分析及预警等功能，显著提高了原始数据处理效率。但云端产生的任何风险都可能引发连锁反应波及被审计端和审计终端，因此云端风险分析及控制直接关系到整个审计任务的效率和效果。

1. 从数据安全性来看，云端主要面临数据存储

风险和数据隔离风险。数据存储风险主要是指被审计端上传的原始数据外泄以及云端遭受外围黑客或病毒攻击，对原始数据的完整性、真实性、准确性产生的负面影响。由于被审计端通过网络接口技术按期将原始数据上传至云端，云端利用虚拟化技术将数据存储在不同服务器上，导致原始数据准确存储位置无法定位，对于部分敏感性和重要性原始数据无法针对性地实施加密保存，进而加大了某些重要性原始数据外泄的风险。同时，被审计端的数据存储和审计终端的数据处理相关的逻辑控制和物理控制都严重依赖于云端，而云端外围网络环境的不稳定性（如遭受黑客或病毒恶意攻击）会对原始数据的完整性、真实性、准确性产生负面影响，进而加大云端的数据存储风险。

数据隔离风险主要是在云服务共享环境下，云端在数据管理和用户数据分配过程中出现混乱可能产生的风险。特别是在公共云下，审计终端和被审计端只是云端客户群体之一，云端也可能为其他用户提供数据存储和计算资源，这就导致云端同时为多个用户提供不同类型数据存储和分析服务，如果各用户存储数据不能实现有效隔离，可能会给审计原始数据带来安全隐患。

2. 从云审计系统应用来看，云端主要面临访问控制无效风险、平台共享风险及平台传输风险。首先，就访问控制无效风险而言，在共享环境下不同用户可以通过访问控制和身份识别登录云端，享受相关云计算服务，而常用的访问控制和身份识别大多采用账号密码等传统登录设置，这容易引发由于登录账号及密码被盗、因密码等级低而被破解等产生的非法登录风险，一旦被审计端或审计终端访问控制被非法侵犯，就会对云端审计数据的安全性、完整性和准确性产生重大影响。因此，如何对云端实施审计作业的访问者进行有效身份识别，已成为云端保证审计数据安全的关键屏障[3]。

其次，虽然云端服务商能够同时为多个用户提供基础设施、应用软件及计算资源等服务，但是云计算资源的共享也导致了平台共享风险的增加。尤其是云端基础设施服务底层组件未能采取有效的隔离措施对不同用户间应用程序运行及数据运算资源进行有效分离，可能会引发不同用户间应用程序的相互干扰，也为不法分子恶意干扰、破坏审计终端审计作业提供了机会。

最后，云端提供的强大数据处理服务及应用程序的快速运行都需要高速、稳定、便捷的网络宽带传输平台作为前提条件。尤其是审计端对原始数据频繁的调取、信息交换以及数据存储，都对云端宽带传输负荷提出了更高的要求。一旦云端网络传输超负荷运行，将引发传输风险，进而导致审计终端无法正常开展审计作业，影响审计计划的顺利实施[3]。

（三）审计终端风险分析

云端为审计终端提供的智能化数据处理能有效实现对被审计端的远程监督，相比于传统的审计技术与方法，云审计为审计终端提供原始数据分析报告及预警结果报告，能够为现场审计指明审计重点和审计方向，有效提高了审计效率和审计质量。但审计终端对云端数据处理的过分依赖，也使其面临着诸多风险。

1. 在审计人员方面，存在专业胜任能力不足与违规操作风险。就专业胜任能力而言，云审计是将云计算提供的诸多服务应用到审计工作实践中，预期审计效果的实现取决于审计人员的专业胜任能力，一旦审计人员的专业素质和技能无法适应云审计工作要求，将对审计效率和审计质量产生负面影响。因此，想要有效应用云审计工作成果，不仅要求审计人员掌握审计业务专业知识，还要对计算机技术、网络应用技术以及软硬件系统具有充分了解。但受制于传统审计思维和操作方式，审计人员缺乏对云计算技术、计算机审计等知识的了解，在实际应用过程中可能因胜任能力不足而导致擅自修改系统设置、数据处理不当等问题。同时，云审计作为审计技术的优化创新，应针对性地提供相应的应用指南和准则体系加以引导。而传统的准则体系及应用指南仍局限于传统审计技术，难以解决新环境下云审计实践应用过程中遇到的问题。这使得审计人员在专业胜任能力上本就存在瑕疵的前提下，仍然面临缺乏标准技术规范体系和应用指导的困境，进而导致审计人员违规操作风险增加，审计失败风险骤增。

2. 现场审计面临着审计证据缺失和审计程序无效两种风险。传统审计技术能够通过现场查阅、盘点等方法获取适当的审计证据，但是在云审计应用过程中，审计终端通过登录云端直接查阅被审计端上传的电子数据，审计数据分析报告和预警结果报告也是依靠云端智能化处理得出，审计终端只能以此指导现场审计，难以将其作为充分、适当的审计证据。因此，审计证据的缺失在一定程度上增加了现场审计失败的风险。此外，虽然云端能够高效处理海量

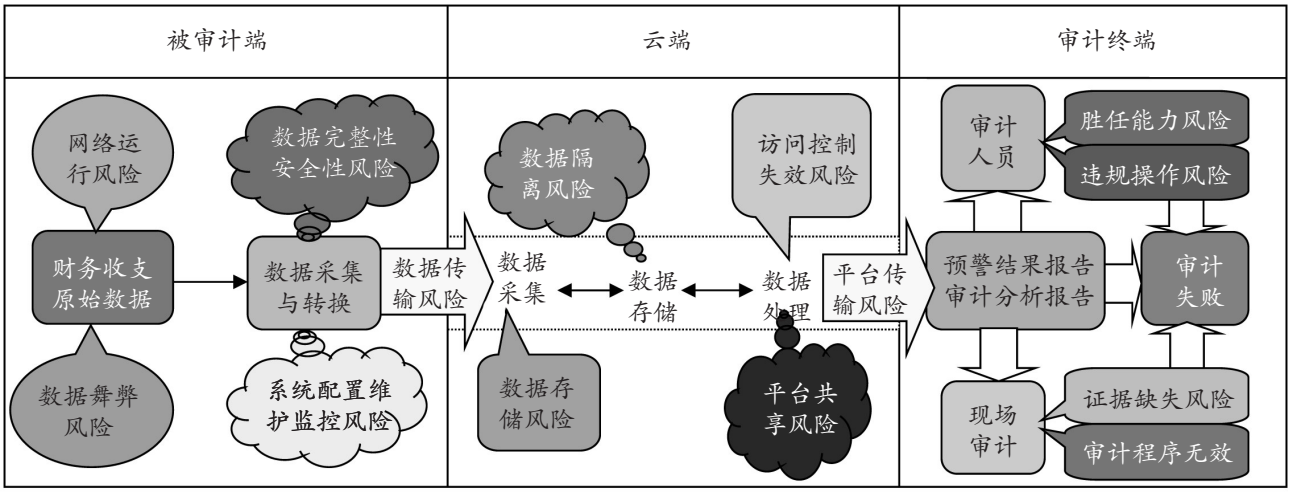

图 3 云审计系统应用风险

数据并得出数据分析报告与疑点预警报告，为现场审计指明方向和重点，但是该结果仅是基于原始数据分析得出的，审计终端无法通过云端对被审计端内部控制设计及执行的有效性进行充分评估。如果被审计端内部控制存在重大缺陷导致其原始数据采集的完整性和准确性存在问题，将会直接影响云端上传的数据分析报告和预警结果报告的可靠性和科学性，最终误导现场审计，致使审计程序无效或审计失败。

综上所述，云审计系统的应用风险及其传导过程如图3所示。

五、云审计系统应用风险控制

（一）被审计端风险控制

1. 优化网络运行环境。被审计端网络运行环境的安全性和稳定性是保证原始数据采集完整性和准确性的第一道“防火墙”。为此，应先搭建完备的安全监控体系（如非法入侵、病毒防护、防火墙等技术），对被审计端网络运行环境进行周期性防御，以防止黑客或病毒产生的威胁。同时，引入互联网物理隔离技术，当被审计端网络安全遭受威胁时，能够通过加密验证对访问者身份进行有效识别，并构建隔离模型对不同安全级别网络进行有效分离，以保证数据采集源头不受外围网络的威胁和干扰。

2. 建立远程访问监控系统。被审计端系统自带的操作日志能够准确记录登录者身份、登录时间和登录地点等事项，这为远程访问监控系统、准确定位登录人员具体操作行为和权限提供了基础。通过将系统操作日志记录的操作事项与远程访问监控系统对特定访问主体设定的操作权限对比，能够有效识别并实时监控非法访问和非法操作，防止被审计端数据采集过程中可能存在的数据舞弊风险。

3. 做好基础设施定期维护检测工作。海量数据的实时采集与频繁更新对被审计端基础设施的稳定性提出了更高的要求，尤其是内存设备和系统异常清除方面。被审计端应统一管理不同存储设备并利用虚拟化技术保证内存设备容量的充足性，同时通过漏洞检测技术、访问控制保障网络服务器运行的稳定性。如若因为内存不足或服务器稳定性不佳导致死机、系统瘫痪、系统不兼容等问题，应及时采取系统运行异常清除技术，以释放系统资源、扩充系统运行空间。

4. 加强数据加密控制。为有效防止被审计端原始数据上传产生的传输风险，可以采用被审计端内部局域网将数据传输至云端，并在数据传输转化过程中加强数据加密与保护，对汇总后准备上传至云端的原始数据进行编码，以产生不可理解的密文，只有通过密码验证才能查阅原始数据。该举措不仅能够防止原始数据外泄，还能防止云端后台人员对数据进行人为删减，有效保证了数据的完整性和安全性。

（二）云端风险控制

1. 加强设备安全配置管理，以控制数据存储风险。系统安全配置管理能够有效提高云端在复杂环境下的数据存储、备份和恢复能力。远程https协议传输与命令行相结合，显著加强了设备安全保障，不仅能够监控云端网络环境稳定性以及软硬件设备运行状态，还能够在外界威胁、干扰环境的情况下自动保持、备份原始数据，即使遭遇病毒或黑客攻击，也能在指定端口实现数据恢复。

2. 利用智能探针与分析提取技术实现数据隔离并控制平台共享风险。智能探针是将不同类型数据打上差异化污点标签以进行分类管理，能够实现不同等级和性质数据的分离存储。同时，污点标签的存在不仅能够准确定位指定数据的存储位置和动态，还能记录和保存针对该数据相关的操作日志，有助于提高数据分离存储的安全性。此外，对于云端存储的数据规模和使用价值而言，有效识别使用频率较高和价值密度较高的数据显得尤为重要。为此，可以采用大数据分析提取技术识别不同数据使用价值，针对性地减小高价值数据共享应用程序和资源之间的相互影响，以有效控制平台共享风险。

3. 加强登录访问控制。在云审计系统中，审计终端和被审计端均通过访问登录实现审计作业，如何保证两个端口访问者身份的合法性，成为云端访问风险控制的关键环节。为此，云端可利用双密码管理与同一身份认证相结合，以有效控制非法登录风险，即采用固定账号密码登录设置与特有标识码设置（如短信提醒、指纹识别或特殊标识等）相结合的双密码管理，对同一身份认证进行双向检验。

（三）审计终端风险控制

1. 不断提高审计人员专业胜任能力。云审计的广泛应用对审计人员专业胜任能力提出了更高要求，为更好地利用云审计开展审计相关作业，应重点加强对审计人员的素质培训。培训内容既包括审计专业技能，还应包括计算机技术、网络应用技术以及软硬件设备等内容，通过持续的素质培训与云审计实践相结合，不断提高审计人员驾驭云审计的实践能力和胜任能力。同时，还应在实务中成立专门的指导小组，帮助其解决云审计实际应用过程中遇到的难题，使得更多审计人员能够尽快适应云审计发展要求。

2. 采取远程审计与现场审计相结合的循环审计模式。云端不仅有效释放了被审计端数据存储空间，还为审计终端直接利用云端智能化数据处理服务提供了有利条件，但是云端针对原始数据分析得出的结果以及预警报告的可靠性和科学性仍需要现场审计加以检验。通过远程与现场循环审计，了解被审计端原始数据采集内部控制设计与执行情况，以此判断云端数据分析报告和预警结果的可靠性。同时，利用编程技术和建模思路将远程审计与现场审计所得经验固化成相应数据库，为审计人员后续开展连续审计提供参考经验。

综合以上分析，云审计系统应用风险控制对策整理如图4所示。

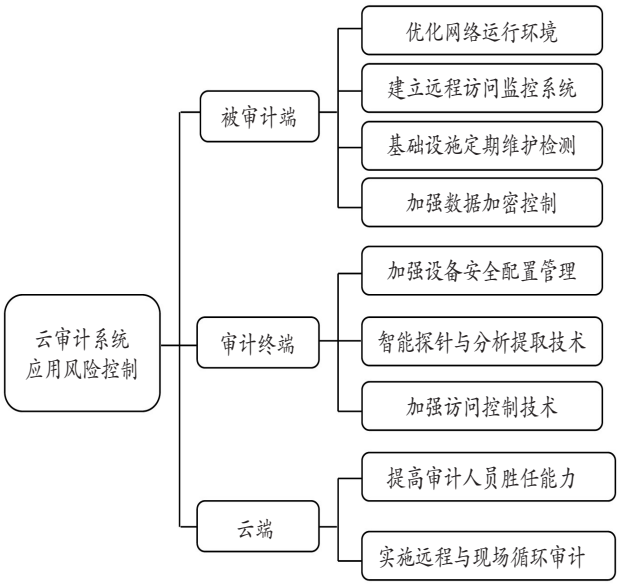

图 4 云审计系统应用风险控制对策

主要参考文献：

[1] 乔冰琴. 云计算在软件测试教学中的应用研究[J]. 山西财政税务专科学校学报，2014(2)：72～74.

[2] 丛秋实，黄作明，张金城. 协同国家审计的实现路径研究：基于云审计[J]. 当代财经，2014(10)：120～129.

[3] 钱瑞，王帆. 大数据时代下社保基金云审计风险控制研究[J]. 财会研究，2017(4)：59～64.

作者单位：1.湖北文理学院经济管理学院，湖北襄阳 441053；2.香港大学教育学院，香港 999077