基于数字化审计管理系统模式的改革研究

张 晶,李 杰,景嘉伟,刘志源
(国网甘肃省电力公司,甘肃 兰州 730030)

摘 要:研究数字化审计管理机制的新型构建模式并实现管理技术升级。将部署在审计现场的临时云系统整合到私有云中,实现对审计机关 IDC 的升级,在软件层面使用计算机辅助系统代替常规的程序化审计过程,包括对流水账的梳理过程、银企对账单的确认过程、审计报告的编制过程等。系统升级后,审计机关工作人员从 12 人压缩到 5 人,且审计机关用于具体审计工作的人均工时从 215.0 小时降低到 117.6 小时。同时,经过专业网络安全评估机构的评估,审计系统数据安全性也得到了有效提升。数字化审计管理机制的升级可以有效提升企业内部审计的工作效率和工作质量,对审计数据的安全保障也有实际意义。

关键词:数字化审计;管理信息系统;审计大数据;审计效率;审计质量
中图分类号:TP393.07;TM425 **文献标识码**:A **文章编号**:1673-629X(2021)0198-04

Research on Construction of Digital Audit Management Mechanism

ZHANG Jing, LI Jie, JING Jia-wei, LIU Zhi-yuan
(State Grid Gansu Electric Power Company, Lanzhou 730030, China)

Abstract: To study the new construction mode of digital audit management mechanism and realize the upgrading of management technology. The temporary cloud system deployed in the audit site was integrated into the private cloud to upgrade the IDC of the audit institution. At the software level, the computer-aided system was used to replace the routine programmed audit process, including the sorting process of the convection water account, the confirmation process of bank enterprise statement, the preparation process of audit report, etc. After the system was upgraded, the number of audit staff was reduced from 12 to 5, and the average working hours of audit institutions for specific audit work decreased from 215.0 hours to 117.6 hours. At the same time, after the evaluation of professional network security evaluation institutions, the data security of audit system has also been effectively improved. The upgrading of digital audit management mechanism can effectively improve the efficiency and quality of internal audit, and has practical significance for the security of audit data.

Key words: digital audit; management information system; audit big data; audit efficiency; audit quality

0 引 言

提升审计工作质量的关键切入点在于获得真实、可靠、有效的审计数据。从审计目的来看,包括国家审计部门对国有企业的审计和投资方对子公司的审计等基于股权管理权的审计目的,企业发行债券、基金或完成上市、不良资产交易、大数据资产交易等基于风控管理需求的审计目的,合资项目中基于项目权责确认和分割等审计目的。这些审计过程都需要对原始账目信息进行妥善管理。

但是,传统审计过程必须从被审计方财务及经营管理部门获得审计原始资料,被审计方出于获得更有优势的审计结果的目的,可能会提供不完整的审计原始资料甚至提供经过更改的审计原始资料,这使得审计工作长期以来难以完全反应出被审计方的真实状态。所以,在国家审计署等单位的促进下,进入 21 世纪以后,数字化审计工作在国内得到推广。

数字化审计的本质是实现数据的联动性,即被审计方向税务、统计等所有部门报送的各类报表及相关原始资料均会在数字化审计体系下实现共享。此举会避免被审计方的“内外账”问题,有助于在本质上提升审计质量。文中梳理研究近年来的数字化审计实现模式,探头数字化审计工作的进一步提升方法。

1 数字化审计的管理信息系统

当前,国家审计部门采用的数字化审计系统一般由三层架构构成。主要为:审计机关内部部署的 IDC 机房设施,以及审计现场部署的临时审计办公网络,共同形成数字化审计物理层;由现场审计的相关数据和

收稿日期:2021-03-23
作者简介:张 晶(1985-),男,硕士,高级工程师,高级经济师,研究方向为数字化审计。

审计机关内部的备份数据及衍生数据构成的数据层;审计过程使用的各种软件系统构成的应用层。而民营企业的审计部门,也多沿用了这种数字化审计的管理模式,详见图 1。

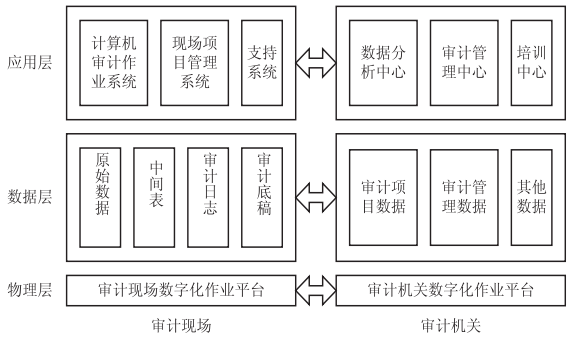

图 1　数字化审计管理信息系统的一般模式

图 1 中,物理层是审计数字化系统运行所必需的硬件环境,包括网络、服务器、终端以及移动存储设备等;数据层用于存储审计中所产生和使用的各种数据,它在逻辑上相对独立于应用系统,并采用元数据管理方式进行管理,以保证数据的一致性和使用上的便利;应用层由各个具体的应用系统所组成,其中不仅包含软件系统,而且包含各个具体应用的操作规程、管理策略等。

物理层是审计工作展开的基础,当前审计工作的工作需求以及当前投资环境使得子公司内部的经营管理系统、财务系统普遍与母公司联网,母公司审计部门可以将大部分财务审计工作和部分专项审计工作从被审计方转移到母公司审计机关内直接执行。即在民营企业的审计工作中,审计现场的大量智能向审计机关转移。

所以,图 1 中审计现场和审计机关的管理信息系统边界逐渐模糊化,形成一种互联网+审计的工作系统,详见图 2。

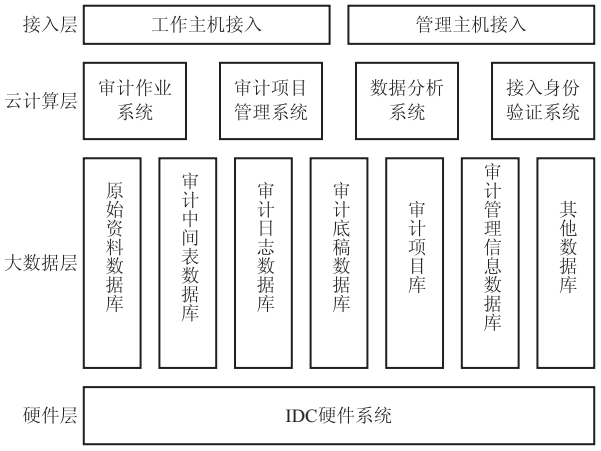

图 2　互联网+审计的数字化审计管理系统革新

图 2 中,审计现场的数字化审计系统与审计机关的数字化审计系统融合到审计机关内部署的 IDC 硬件系统平台上,在 IDC 中部署数据仓库系统用于对数据整合管理,部署云计算系统将审计用软件系统全部部署到云端,而使用通用计算机设备在接入身份验证系统的安全保护机制下直接使用 WEB 浏览器接入审计系统,如在审计机关具有局域网条件的,可直接使用局域网接入,而在审计现场没有局域网条件的,可以在公共互联网上使用 VPN 链接接入。

2　审计数据的安全保障

审计过程中会涉及到大量涉密财务数据和涉密管理数据,如何在审计过程中充分保障数据的安全性,是当前数字化审计管理信息系统的重要功能需求。在互联网+审计管理模式中,使用以下两点完成对审计数据安全的管理任务。

2.1　严格的身份识别机制

传统的管理信息系统身份识别模式,一般采用 POST 用户 ID 及密码的方式实现身份识别,稍高级的身份识别模式可能用到外置加密设备实现身份识别,但不论采用哪一种身份识别模式,均存在一定的泄露风险,比如用户 ID 和密码的身份识别方式仅可以实现对用户 ID 和密码的识别,并不能证实是用该用户 ID 登录的用户是否为对应的审计人员本人,外置加密设备同样有此问题。所以,为了充分确保使用者身份,数字化审计系统的身份识别模式,应采用综合身份识别方案,详见图 3。

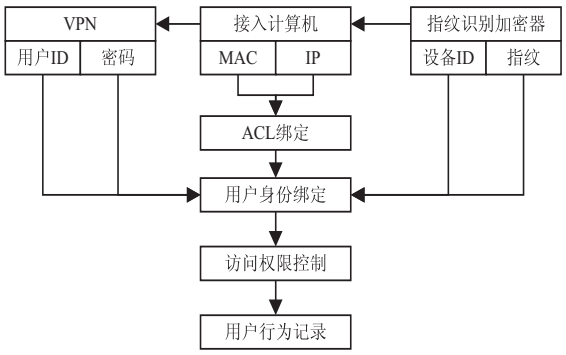

图 3　数字化审计管理系统的身份识别方案

图 3 中,使用计算机网卡(IC)的 MAC 地址与 IP 地址的绑定来确认计算机的接入许可,不能满足该 ACL 绑定的计算机,无法在局域网中获得任何信号服务。而此处的 MAC 地质标定的计算机,与指纹识别加密器的设备 ID 之间形成绑定,即特定指纹识别加密器只能在特定的计算机上使用,将计算机 MAC 地址、指纹识别器 ID、用户指纹信息三项信息进行绑定,用于局域网内访问的身份识别,将进一步融入 VPN 的用户 ID,用于外网访问的身份识别。在这种综合身份识别体系下,特定用户的指纹信息必须在特定计算机上使用特定的指纹识别加密器进行指纹输入,才可以获

得对应的权限。这一信息安全管理方案可以有效提升用户身份识别的可靠性、私密性、独立性。

2.2 完善的数据仓库机制

数据仓储管理机制包括数据仓促阶段的安全性和数据传输阶段的安全性。基于 VPN 数据的加密封装机制,让数据在公网传输过程得到充分保护,且在数据仓库主机的保护中,严格使用管理员密码、数据库密码、内部数据加密密码、存储介质密码等保护措施,让数据仓库管理机制得到全面安全保障,详见图 4。

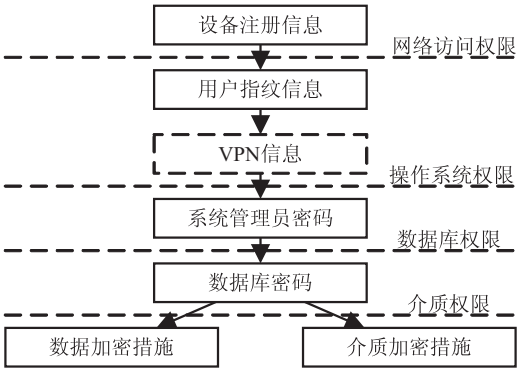

图 4 数据仓库管理机制示意图

图 4 中,用户获得访问数据库的权限,需要使用完整登记的设备(计算机、指纹识别器)等获得网络访问权限,在完整登记的设备上输入指纹信息并使用指定的 VPN 账号登录(外网条件下)以获得操作系统权限。对系统管理员来说,在 IDC 内进行数据仓库的操作,需要有系统管理员密码和数据库密码才可以绕过 PHP 系统外壳进行数据库的 SQL 操作,而如果绕开数据库直接下载数据库内信息,还会受到数据加密措施和介质加密措施的双重限制,即在数据库中,必须确保数据在指定的数据仓库主机且运行指定的逻辑数据库管理软件才可以实现数据的读写和查阅,特别是介质加密措施限定了数据必须在指定硬盘介质上访问,被强制拷贝离开指定硬盘介质的数据,无法被有效打开。

3 审计效率与审计质量的管理与促进

数字化审计管理信息系统的本质是提升审计效率和保证审计质量,所以,革新数字化审计管理信息系统时,必须以提升审计效率和审计质量为核心目的。根据前文分析,改进后的系统会将被审计单位的财务、经营数据信息进行同步,实现数据的远程管理,此时,该审计 IDC 系统的数据接入方式需要有所革新。革新后的 IDC 接口系统,见图 5。

图 5 中,将所有云端功能进行整合并全部置入位于审计机关的私有云 IDC 后,被审计单位的数据会通过 API 虚拟链接实现与 IDC 元数据库的实时同步,在对元数据库信息进行验证后,数据被同步到中央数据仓库中,而所有审计行为均通过中央数据仓库实现。此时,审计工作的划分仍然分为审计机关的相关工作和审计现场的相关工作。但其变化主要有以下两点:

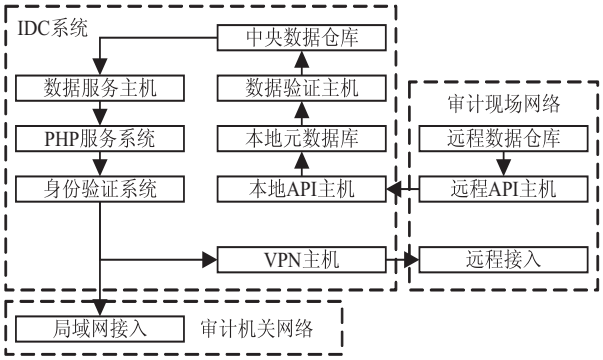

图 5 审计机关 IDC 的接入管理系统

第一,原本需要在现场进行的流水账目清理、财务报表确认、银企对账等程序化工作,被移交到审计机关处理,而且大部分程序化工作实现了计算机辅助处理,一方面使审计现场的工作量充分减轻,另一方面使审计工作更多倾向于获取审计证据。在此改进后,审计人员进入审计现场时,已经获得了上述程序化工作的初步审计结果,在审计现场可以直接进入获取关键审计证据的工作流程中。

第二,审计机关的管理工作从早期的审计结果确认和审计报告编制等,转化为对审计人员行为的管理。而审计结果确认和审计报告编制等工作,也可交由计算机辅助系统完成。

之前审计工作中,程序化工作占据了工作量的绝大部分,审计人员在审计现场对财务流水账和银企对账的人工确认工作,对审计报告的编制工作是早期审计工作中的最大工作量。而根据二八法则,上述占据审计工作 80% 工作量的工作只能提供 20% 的工作价值。节约该 80% 工作量可以有效促进审计效率并提升审计质量。

4 数字化审计管理信息平台的应用效果

个案研究针对某民营企业的内部审计工作,该企业投资子公司 7 个,对外合资项目 4 个,常规审计包括对 7 个子公司和 4 个合资项目的年度常规审计工作。另外,该公司在股权上市、企业债发行、数据资产交易等方面有专项审计需求。该企业财务部门下成立自营审计机构,职能等同于国有企业的审计机关。

该个案企业 2018 年底采用上述方式实现数字化审计管理信息系统的升级,所以,对比系统升级后 2019 年审计工作的实际结果与系统升级前 2018 年审计工作实际结果,可以评价该升级策略的实际应用效果。

在审计效率的评价方面,其审计工作结果见表 1。

表 1　审计效率提升情况

比较项目	审计报告数	投入人员量	现场工时	机关工时
2018 年	17	12	744	1 836
2019 年	19	5	236	352

表 1 中,2018 年共出具审计报告 17 册,其中常规审计报告 11 册,专项审计报告 6 册,审计部门工作人员投入 12 人,总工时 2 580 小时,人均审计工作年工时 215.0 小时。2019 年共出具审计报告 19 册,其中常规审计报告 11 册,专项审计报告 8 册,审计部门工作人员投入 5 人,总工时 588 小时,人均审计工作年工时 117.6 小时。可见,进行管理信息系统升级后,审计部门用于现场审计和编制审计报告的工时数显著降低,审计部门的工作人员定岗定额也可以有效压缩。审计部门可以将更多时间用于企业的运行监控中。

考察数字化审计管理信息系统的安全性,选择专业网络安全机构评估的方式,即使用常规攻击法获得系统的安全性指标。其评价结果见表 2。

表 2　系统安全性评价结果

比较项目	数据暴破时间	DDos 承受能力	侦听数据暴破时间
2018 年	45.6 h	5.3 h	27.4 h
2019 年	>3 000 h	36.4 h	157.2 h

表 2 中,网络安全测试机构拷贝硬盘数据后进行暴力破解,升级前系统的暴破时间为 45.6h,而升级后系统经过 3 000 h 暴破后,并未读取解密信息。采用 30 k 节点进行的 DDos 攻击中,升级前系统经过5.3 h 系统崩溃,而升级后系统经过 36.4 h 系统崩溃,抗 DDos 攻击能力提升 6.9 倍,该 36.4 h 抵抗窗口内,安全管理人员可以获得充足时间发现攻击源并作出对策。对 POST 信息进行侦听并获得数据报文后,升级前系统的成功暴破时间为 27.4 h,而升级后系统的成功暴破时间为 157.2 h。同时,该测试还对系统进行了注入式攻击、扫描攻击等攻击测试,系统升级前后对该两项攻击均做出有效防范,故不在上述对比中进行比较。

可见,该系统在 IDC 内的数据安全保障具有较强安全性,其安全短板在数据 POST 过程中,但仍较升级前将侦听数据暴破时间提升了 5.7 倍。

5　结束语

本次对数字化审计管理信息系统的核心升级思路,是将部署在审计现场的临时云系统整合到私有云中,实现对审计机关 IDC 的升级,在软件层面使用计算机辅助系统代替常规的程序化审计过程,包括对流水账的梳理过程、银企对账单的确认过程、审计报告的编制过程等,使现场审计人员可以将更多精力放在审计证据的获取工作中。软硬件进行综合升级后,共有三个效果表现:

(1)提升了系统安全性和数据安全性,确保审计过程中敏感数据泄漏的可能性被最大限度压低。

(2)提升了审计工作效率,系统升级后,审计机关工作人员从 12 人压缩到 5 人,且审计机关用于具体审计工作的人均工时从 215.0 小时降低到 117.6 小时。审计人员可以将更多精力放到企业运行状态的监控中。

(3)提升了数据真实性。通过 API 整合子公司和合资项目的财务管理系统、经营管理系统后台数据后,审计工作实现了自动化和实时化,审计过程受到被审计单位人为影响的可能性被压缩到最低。

参考文献:

[1] 刘高原,张永强. 基于系统论的企业内部数字化审计体系研究[J]. 中国内部审计,2020(8):22-26.

[2] 蔡　玺,李　兴,祝唯微,等. 基于大数据的电力营销数字化审计应用研究[J]. 电子世界,2020(14):75-76.

[3] 黄妙红,王　珏,肖嘉丽. 省级电网企业数字化审计平台建设的路径[J]. 管理观察,2020(21):24-25.

[4] 蔡　捷. 探索计算机技术在工程造价审计中的运用[J]. 财富时代,2020(7):182-183.

[5] 陈冬梅,纪永满,肖　丹,等. 基于全业务数据的多维度数字化审计体系构建[J]. 中国内部审计,2020(7):28-35.

[6] 王　威,黄　海. 基于数字化的电网大修工程审计建模应用实践[J]. 中国内部审计,2020(7):44-45.

[7] 田桂申,白雪娇. 电力企业内部审计应对新冠疫情的相关思考[J]. 中国内部审计,2020(7):7-9.

[8] 赵　亮. 机器人技术在数字化审计领域的实践应用[J]. 中国军转民,2020(7):63-65.

[9] 李小牧,李亚萍. 数字化审计视角下电网企业供电所审计质效提升探究[J]. 中国市场,2020(17):151.

[10] 王　峥. 企业内部审计的信息化应用[J]. 电脑编程技巧与维护,2020(6):98-100.