第 3 章

联网审计原理及其关键问题分析

3.1 引言

由前文所述，随着信息技术的发展，审计对象的信息化使得计算机辅助审计成为必然。在我国，为了适应计算机辅助审计的需要，国家审计署已经成功开展了“金审工程”的建设工作。“金审工程”是我国审计信息化的简称，是列入我国电子政务“十五”期间启动的 12 个重大业务工程之一。“金审工程”的建设具有如下意义（国家 863 计划审计署课题组，2006）：

（1）审计信息化象征着审计工作将发生三个转变：从单一的事后审计变为事后审计与事中审计相结合；从单一的静态审计变为静态审计与动态审计相结合；从单一的现场审计变为现场审计与远程审计相结合。

（2）审计信息化必将推动审计方法的改变。对被审计单位的账目逐笔审计在过去是不可想象的，但在审计信息化情况下将轻而易举。

（3）审计信息化必将推动广大审计人员思维方式的转变，增强审计人员的全局意识和宏观意识。

（4）审计信息化必将提高审计质量，降低审计风险。

“金审工程”一期主要完成了硬件建设和部分现场审计软件开发，以及人员的培训等工作。为了探索计算机辅助审计数据采集与处理中的重大技术和制度规范，为“金审工程”二期实施联网审计系统建设提供科技成果应用的指导，国家审计署已成功开展了国家 863 计划“计算机审计数据采集与处理技术”一期课题和二期课题的研究，通过该项目的开展，探索了适合我国国情的联网审计实施方案（国家 863 计划审计署课题组，2006）。本章将在分析我国持续审计（联网审计）实现原理的基础上，针对我国联网审计的特点，探讨实施联网审计过程中面临的若干关键问题，从而为后面研究联网审计的审计取证技术和绩效评价打下基础。

3.2 联网审计原理

如第 2 章所述，目前我国正在开展的联网审计也是持续审计的一种实现方式，它是通过不断地采集被审计单位信息系统中的数据来实现，其在技术实现上主要包括数据采集、数据传输、数据存储以及数据处理 4 个部分。这种方式也可以看成是一种面向数据的联网审计

(Data-Oriented Online Auditing,DOOA)(Chen 等,2007)。其原理如图 3.1 所示。

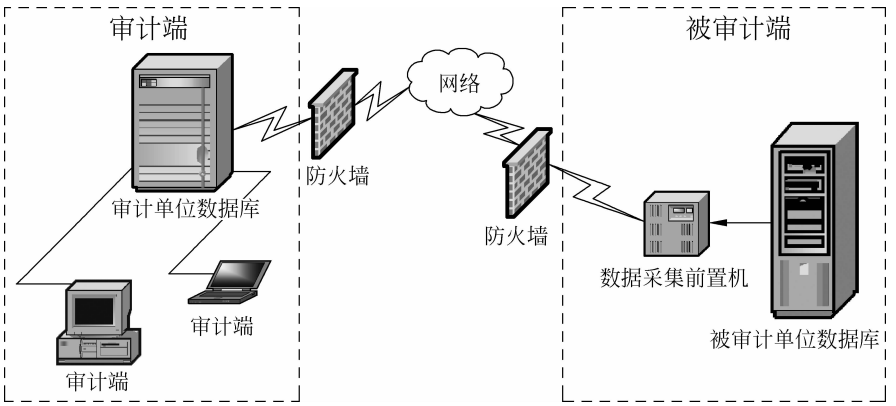

图 3.1　我国联网审计实现方法的原理

1. 审计数据采集

要实现联网审计,必须研究如何采集被审计单位的电子数据。一般来说,联网审计数据采集的实现是通过在被审计单位数据服务器端放置一台称为“数据采集前置机”的服务器,通过在“数据采集前置机”上安装数据采集软件,把审计需要的财政财务数据和相关经济业务数据采集到部署在本地的审计数据采集服务器(前置机)中,从而完成联网审计的审计数据采集工作。

2. 审计数据传输

审计数据传输主要用来把采集来的数据通过网络传输到审计单位中去,以供审计数据分析使用,即利用公共通信资源网构建的联网审计数据传输网把部署在被审计单位审计前置机中的数据传输到审计机关的数据中心。在实际工作中,可以根据具体的情况采取相应的数据传输方式。例如,对于大数据量,且要求实时审计的数据,可以采用专线的方式进行数据的传输;对于多级数据分散存储的单位,可以采用专线、拨号等方式进行数据传输;对于网络设施不太完善的被审计单位,可以采用电话拨号进行数据传输。

3. 审计数据存储

联网审计环境下,由于从被审计单位采集来的电子数据是海量的,因此,对于采集来的电子数据需要采取一定的方式来存储,即可以在审计机关构建联网审计的海量数据存储系统。例如,武海平等(2006)就研究了针对联网审计的海量数据存储方式。随着云计算技术的发展,将来也可以采用云存储技术来解决联网审计环境下审计数据的海量存储问题。

利用海量数据存储系统可以实现按不同的应用(逻辑)或按数据特征(类型)进行分区管理。例如,在海量数据存储系统中,可以根据联网审计的需要或不同数据特征的需要,同时存放税务联网审计、海关联网审计、银行联网审计等若干个系统的海量数据,如图 3.2 所示。

4. 审计数据分析

这一阶段主要是采用相关审计工具和方法对采集来的电子数据进行分析,从而发现审

计线索，获得审计证据。联网审计环境下，采集来的数据是海量的，因此，研究如何分析被审计数据，获得审计证据是实现联网审计的关键。将在第 4 和第 5 章中对这一内容进行研究。

根据以上分析，联网审计可以归纳为：联网审计是由于网络技术在审计中的应用而形成的一种新的审计模式，它通过网络采集被审计单位的电子数据，进行连续、全面的分析，及时发现被审计单位存在的问题，为现场审计提供线索和资料，从而使得审计工作实现网络化、远程化。

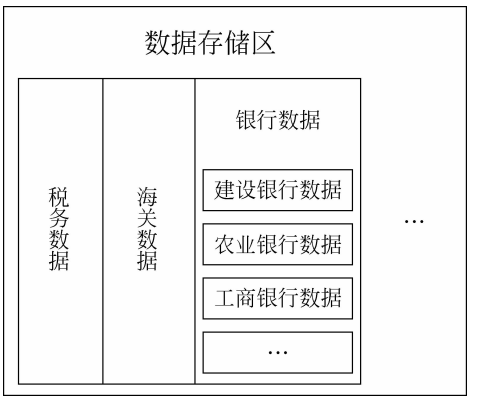

图 3.2 审计数据分区管理示意图

3.3 实施联网审计的优缺点分析

1. 主要优点

根据前文对联网审计原理的分析，实施面向数据的联网审计的主要优点如下：

1）能有效消除 7 种审计浪费

传统的审计模式具有 7 种审计浪费，即过度审计、等待、时间延迟、审计过程自身的无效率、审计过程的不连续、过多的审阅过程、误差，而实施联网审计能有效消除这 7 种审计浪费。比如，减少调阅资料时间，审计人员可以远程获取主要审计资料，避免传统审计中依赖被审计单位提供数据，等待数据的时间。根据统计，一般审计项目中，审计人员等待调阅会计资料的时间大量占用审计人员的有效工作时间。联网审计模式下，主要的审计数据采集是通过数据采集前置机来获得的，具有前所未有的主动性和灵活性。

2）降低了审计成本

实施联网审计后，需要的相应审计人员会减少，降低了审计人员相应的成本。对于异地审计项目的审计，实施联网审计能有效地减少外勤经费，如差旅费、住宿费等，这也大大降低了审计成本。

3）节省了审计的时间，提高了审计效率

传统审计模式下，由于审计对象的情况往往比较复杂，仅凭一次审计就把全部问题都查出来几乎是不可能的。而采用联网审计则可以把数据采集来之后，采用先进的数据分析方法对被审计数据进行仔细的分析，从而可以全面发现审计线索。

4）提高了审计的独立性

审计人员依赖被审计单位提供数据，现场审计时，提供数据的效率和质量影响到审计行为的实施效果。联网审计时，借助于联网审计系统，审计人员具备更大的灵活性和行为的独立性。可以对审计事项进行更加自由的调查取证，形成审计意见。此外，现场审计时，审计人员和被审计单位人员在工作全过程中接触，在涉及敏感问题时，难免会受到各方面的干扰，影响到审计人员的独立判断。而在联网审计模式下，审计人员与被审计单位人员处于物理上的不同地点，从环境上有利于审计人员的独立性。

2. 主要缺点

根据前文对联网审计原理的分析，实施面向数据的联网审计的主要缺点如下：

1）实施成本高

实施联网审计的成本可以分成一次性成本和经常性成本两部分。一次性成本是指联网审计系统开发和执行的初始投资；经常性成本是指在联网审计系统整个生命周期内反复出现的运行和维护成本。

针对目前我国联网审计的实施方法，其一次性成本主要包括：

- 硬件成本；
- 软件成本；
- 人员培训费用；
- 场地成本。

针对我国目前联网审计的实现方法，其经常性成本主要包括：

- 人员成本；
- 硬件维护成本；
- 软件维护成本；
- 耗材成本；
- 风险控制费用；
- 其他费用，如网络通信费等。

对于实施联网审计的成本，将在第 6 章进行详细分析。

由联网审计的成本构成可以看出，实施联网审计的成本是比较高的。因此，在实施联网审计时需要从成本和效益的角度进行可行性研究。

2）技术要求高

联网审计主要是采用信息技术来完成。为了保证联网审计过程的顺利完成，审计人员对联网审计的各个环节，例如审计数据采集、审计数据传输、审计数据存储、审计数据分析等有足够的认识，这就要求审计人员需要具备软件、硬件、网络和数据库等方面的知识。

3）审计风险高

联网审计环境下，审计的主要对象是从被审计单位信息系统中采集来的原始数据，如果被审计单位没有健全的内部控制制度来保证其数据信息的真实性，那么审计人员的工作都将建立在虚假信息之上，带来极大的审计风险。

另外，由于联网审计也是一个复杂的系统，有时灾难性的事故是无法预防或规避的，这些灾难造成的系统停顿也将给审计工作的进行带来重大影响。

3.4　联网审计系统的安全分析

对于图 3.1 所示的面向数据的联网审计系统，其安全控制非常重要。面向数据的联网审计系统的安全因素主要包括审计数据采集安全、审计数据传输安全、审计数据存储安全和审计数据分析安全。

1. 审计数据采集安全

审计数据采集安全主要包括数据采集物理安全、数据采集身份认证与授权，以及审计数据完备性等。

2. 审计数据传输安全

联网审计系统一般需要异地传输大量的数据，其中大部分数据是关系到被审计单位利益的重要数据，有些数据甚至关系到国家的重要利益，而目前联网审计系统的数据传输过程中会涉及公网系统，因此，联网审计系统数据传输的安全性问题非常重要。只有保证了数据传输过程中的保密性和完整性，才能保证系统数据不被截获、不被泄露、不被监听和复制。审计数据传输安全主要包括信息传输安全、传输通道安全和网络结构安全。

3. 审计数据存储安全

在联网审计系统的数据中心存储着大量审计数据，包括从被审计单位采集来的审计数据以及审计人员分析处理后的结果数据，这些数据会涉及被审计单位的敏感信息以及国家的重要保密信息，如果这些信息发生泄露，会严重的影响到被审计单位和国家的利益。

另外，数据的完整性也是极为重要的，一旦重要数据被破坏或丢失，就会对联网审计系统的日常运行造成重大的影响，甚至是难以弥补的损失。因此，审计数据存储的安全也很重要。

审计数据存储安全主要是要保证审计数据的连续性、共享性和可使用性，同时要保证审计部门内外数据的安全隔离。另外，为了防止各种灾难给数据存储带来的损害，应该建立异地备份方案。审计数据存储安全可通过实施业务持续计划(Business Continuity Plan，BCP)完成，对于这一内容，将在 3.5 节分析。

4. 审计数据分析安全

审计数据分析安全主要包括审计人员在进行审计数据分析的过程中，不能更改原始的被审计数据，不能泄露相关的被审计数据等。

3.5 基于 BCP 视角的联网审计风险控制

3.5.1 问题的提出

目前，对于联网审计的研究多是从技术实现的视角出发，很少研究联网审计的风险控制问题。然而，联网审计也是一个复杂的系统。有时灾难性的事故是无法预防或规避的，这些灾难造成的系统停顿也将给审计工作的进行带来重大影响。如果有对意外事件的详细规划，就可能避免灾难和系统停顿的全面影响，而 BCP 则是解决该问题的最佳方案。基于以上分析，可以看出从 BCP 的视角研究联网审计的风险控制具有重要的理论和应用价值。

3.5.2 BCP 原理

1. BCP 的概念

业务持续计划是单位为避免关键业务功能中断，减少业务风险而建立的一个控制过程，它包括了对支持单位关键功能的人力、物力需求和关键功能所需的最小级别服务水平的连续性保证(James 等，2000)。BCP 关注的是单位日常风险管理程序所不能完全消除的剩余

风险，BCP 的目标就是要把单位的剩余风险和因意外事件产生的风险降到单位可接受的程度。一般来说，业务持续计划包括：

（1）灾难恢复计划(Disaster Recovery Plan，DRP)，用来恢复不可用的设备。

（2）作业计划，恢复发生的同时业务单位所应进行的作业。

（3）重建计划，用来将运营恢复正常，无论是旧设备修复还是采购新设备。

2. 制定 BCP 时需考虑的问题

（1）制定 BCP 的第一步是进行风险分析，即识别风险。通过评估一个单位的信息资源所存在的威胁，了解每一个风险可能会造成多大的损失，然后采取适当的措施把相应的风险减少到单位的高级管理层能够接受的水平。需要指出的是，并不是所有的系统都需要一个恢复计划，业务持续计划所花费的代价不能超出恢复系统所带来的利润。

（2）BCP 计划的范围和所需要的详细措施依据不同的单位而要求不同。比如，具有大的 IT 部门和复杂的计算机系统的单位应具有一个综合的、不断更新的 BCP 计划，并有相应的备份设施。

（3）BCP 计划应该文档化，并根据需要定期检测和更新。为了检测 BCP 计划是否和期望的一样正常地工作，需要采用灾难模拟练习来定期检测。

3.5.3　联网审计系统的风险分析

为了保证联网审计的连续，从而有效地对被审计单位进行实时监控，根据 BCP 的思想，首先需要分析联网审计系统的风险。根据对联网审计的原理以及联网审计系统的 4 个主要组成部分的分析，其数据采集部分、数据传输部分以及数据存储部分是风险控制关注的重点，其中数据存储部分最为重要，而数据采集部分和数据传输部分的重要性取决于联网审计的频率。另外，被审计单位的特点以及联网审计系统的规模也是产生风险的关键。

在实施联网审计时，应当采取合理的、具有可接受的恢复成本的风险控制方案，即联网审计的恢复成本不应大于停机成本。

3.5.4　联网审计系统的风险控制方案

1. 数据采集部分的风险控制

为了防止联网审计的数据采集部分由于灾难等造成的系统停顿，对于数据采集部分，主要是做好数据采集前置机中相关软件系统及关键数据的备份工作，包括数据采集软件系统、审计预警系统的备份工作。可以把相关需要备份的软硬件系统备份到实施联网审计的审计单位和当地的审计部门中。当被审计单位发生灾难时，可采用备份在当地的审计部门中的数据快速恢复数据采集系统。当发生大范围的灾难时，可采用备份在联网审计单位的备份数据来完成恢复。其中，需要注意的关键问题如下：

1）关键应用程序清单的准确性和完整性

审计人员应检查关键应用程序清单以确保其完整性和准确性。应用程序遗漏会导致恢复失败。但是，将实现短期恢复不需要的应用程序列入关键清单，会在恢复期间误导资源，分散对基本目标的注意。

2）注意备份关键应用程序

审计人员要检查关键程序的副本是否非现场存储，这样，一旦发生灾难或系统故障，就可用备用版本重建数据采集系统。

3）注意备份关键数据

审计人员应检验关键数据文件是否按照要求进行了备份。

2. 数据传输部分的风险控制

数据传输是联网审计系统的关键部分，如果不能准确地把采集到的数据传输到审计单位去，则无法完成联网审计。所以，要实施联网审计，保证网络的畅通很重要。对于联网审计的数据传输，主要是预防网络灾难中通信的中断。另外，应当使用足够的不间断电源（Uninterruptible Power System，UPS）设备来保证通信设备的安全供电。通信网络像数据中心的其他设施一样易受自然灾害的影响，特别是有一些灾难事件对通信网络有较大的影响。例如，中心交换设备间发生灾难，电缆被切断，通信软件出现故障与错误，由于黑客入侵造成的安全损害，人为灾祸对主机的破坏等。对通信网络进行保护的主要方法如下：

1）采用冗余设施

主要包括：

（1）在规划通信能力时留有富余，当其主要通信能力丧失时，使用其剩余通信能力。例如在局域网中设计双路电缆，其中一条正常使用，另一条作为备份路径，一旦正常使用的电缆被损坏，就启用备份电缆，保证网络正常连通。

（2）在路由器之间提供多条路径。

（3）提供容错设施，以避免路由器、交换机和防火墙的单点故障。

（4）把网络设备的配置信息复制出来保存，以备恢复时使用。

2）采用替换式通信线路

替换式通信线路是通过一个替换线路来传送信息的方法。

3）采用分集式通信线路

分集式电缆应当处于不同的电缆护套中，而且不能铺设在同一个管道中，它们应当有不同的物理路径，以避免面临同样的灾难事件，这样，分集式电缆才能互为备份。

在实施联网审计时，可根据具体的情况，采取合适的数据传输灾难防范措施。

3. 数据存储部分的风险控制

1）异地备份方法

联网审计的数据存储部分是风险控制需要重点考虑的问题。随着联网审计的开展，审计部门会积累大量的从被审计单位采集来的电子数据，这些数据对审计人员来说是非常重要的。为了防止灾难给数据存储带来的损害，应该建立异地备份方案。各种可能用到的异地备份方法如下：

（1）热站。

热站（Hot Site）提供机房环境、网络、主机、操作系统、数据库、通信等各方面的全部配置，灾难发生后，一般几个小时就可以使业务系统恢复运行。

（2）温站。

温站（Warm Site）只配备了部分设备，通常没有主机，只提供网络连接和一些外部设备

(例如磁盘驱动器、磁带驱动与控制器、UPS设备等)。使用温站是基于这样一个前提：计算机很容易获得,并可以快速安装使用。

(3) 冷站。

为了降低成本,可以使用冷站(Cold Site)。冷站只提供支持信息处理设施运行的基本环境(例如电线、空调和场地等)。

(4) 与其他单位的互惠协议。

单位之间签订互惠协议(Reciprocal Agreements With Other Organization)是指具有相同设备与应用系统的两个单位或多个单位之间互相为对方建立备份的方法。这种方式的优点是成本低,缺点是由于缺乏约束力,经常无法执行。由于这种方法有一定的局限性,一般不常被单位所采用。

2) 风险控制方案

根据以上常用异地备份方法,结合联网审计实施的实际情况,数据存储部分可采取的风险控制方案如下：

(1) 可以在数据采集前置机端和数据存储端互为备份。

由于数据采集前置机端放置在被审计单位中,而数据存储端是在被审计单位中,如此一来,正好可以构成互为异地备份。也就是说,在把采集来的数据传输到审计单位的同时,也把采集来的数据在数据采集前置机端进行备份。

(2) 在各特派办或审计厅之间签订互惠备份协议。

不同单位之间签订互惠备份协议时,一般会遇到系统的不兼容、不容易协调的问题,使得这种方法具有一定的局限性,一般不常被单位所采用,但对于我国的联网审计却是一个很好的方案。因为通过"金审工程"的统一规划建设,在审计署的各个特派办之间的软硬件设备基本相似,这为在他们之间建设异地备份打下了基础；另一方面,通过审计署的协调,能使得在发生灾难时,这种备份方案能顺利执行。对于各省的联网审计项目,其异地备份方案可以在省审计厅的协调下,在省内的各个审计机关或省之间的审计机关之间进行。

(3) 建立可单独运行的热站方式。

在以上两种方式都不可行的情况下,实施联网审计的单位可建立单独运行的热站方式,但这种方式成本较高。

3.5.5　研究联网审计风险控制问题的意义及建议

本节从BCP的视角出发,研究联网审计的风险控制问题,其意义如下：

(1) 在发生各种不可预料的故障、破坏性事故或灾难情况时,能够确保联网审计系统的不间断运行,从而达到对被审计单位持续监控的目的。

(2) 在遇到灾难袭击时,能最大限度地保护采集来的审计数据的完整性和一致性,降低数据的损失,快速恢复应用系统和数据。

另外,对于制定的联网审计风险控制方案,应评估其是否合适,需要考虑的问题如下：

(1) 通过审查以前对联网审计风险控制方案的测试结果,核实风险控制方案是否能有效地确保在出现意外中断后联网审计系统能迅速地恢复。

(2) 通过审查单位的突然事件应对程序以及相关人员的培训和练习情况,评估相关人员在突然事件中的有效反映能力。

(3) 通过检测非现场存储的设施以及它的内容、安全性和环境控制情况,来评估非现场存储是否能满足联网审计风险控制的需要。

(4) 成立联网审计风险控制小组。应清楚地列出风险控制小组成员的姓名、住址以及紧急联络电话号码。另外,要检验联网审计风险控制小组成员是否为在职人员,并了解各自分担的职责。

(5) 不管采用什么样的数据存储灾难防范措施,都要对其备份与恢复操作进行经常性的测试。

3.6 联网审计的多数据源集成问题分析

3.6.1 问题的提出

在联网审计的数据采集和数据存储过程中,面临着多数据源集成问题。这是因为联网审计环境下,采集来的数据来自于不同的被审计单位。由于不同的被审计单位每个数据源都是为了某一特定应用,单独开发、部署和维护的,这就在很大程度上导致数据管理系统、数据模型、模式设计和实际数据的不同。比如:

- 在两个数据源中,同一个相同的字段可能有不同的命名,或者两个不同的字段可能有相同的命名。
- 在一个数据源中,一个字段可能由两列构成,而在另一个数据源中,一个字段可以仅由一列构成。

由于多个数据源中的数据可能会出现不同表示、重复、冲突等现象,另外,每个数据源都可能含有脏数据,当多个数据源集成时,发生在单数据源中的这些问题会更加严重。

为了更好地理解多数据源集成问题,首先以 ERP 系统中的供应商信息为例来说明多数据源的数据集成问题。在表 3.1 和表 3.2 中,两个表示供应商信息的数据表分别来自两个不同的数据源,这两个数据源都是关系数据库格式的,但存在模式和数据冲突。

在模式级上,有命名冲突,如在表 3.1 中供应商编号用 ID 表示,而在表 3.2 中供应商编号用 NO 表示;数据表结构不同,如在表 3.1 中没有“信用等级”和 E-mail 这两个字段,而在表 3.2 中没有“传真”这个字段。

表 3.1 供应商信息 1

ID	供应商名称	法人代表	城市	地址	邮政编码	传真	联系电话	冻结标志
0211	西安汽车制动器厂	陈六	西安	陕西省西安市环城西路北段 127 号	710082	029-4264666	029-4264666	N
1131	重庆新工汽配厂	张三	重庆	重庆市大渡口区钢铁路 66 号	400081	023-68834947	023-68834947	N
0242	西安汽车修配厂	李四	西安	陕西省西安市大庆路 3 号	710082	029-3519107	029-3519107	N

表 3.2　供应商信息 2

NO	供应商名称	供应商分类	法人代表	城市编号	地址	邮政编码	E-mail	联系电话	信用等级	冻结标志
1131	新疆轴承总厂	2	王五	9	新疆乌鲁木齐市北京北路 42 号	830011	wangw@tom.com	(0991)3716017	1	0
1141	西安汽车修配厂	3	李四	4	陕西省西安市大庆路 3 号	710082	lis@tom.com	(029)3519107	1	0
1151	青海汽车配件厂	1	赵六	8	青海省西宁市城东区大众街 69 号	810007	zhaol@tom.com	(0971)8177629	1	0

在实例级上，在表 3.1 中，“城市”这个字段的数据是用具体城市名来表示，而在表 3.2 中，“城市”这个字段的数据是用代号来表示；字段“联系电话”的数据格式不同，在表 3.1 中格式为“××××-××××××××”，而在表 3.2 中格式为“(××××)××××××××”；关于“冻结标志”的数据表示也不同，在表 3.2 中用 0/1 表示，而在表 3.1 中用 Y/N 表示。此外，不同供应商编号的数据(0242/1141)实际上可能指的是同一个供应商，另一方面，不同的供应商用的却是同一个供应商编号(1131)。

经过数据清理，集成后的供应商信息数据表如表 3.3 所示。

表 3.3　集成后的供应商信息

供应商编号	供应商名称	供应商分类	法人代表	城市编号	地址	邮政编码	E-mail	传真	联系电话	信用等级	冻结标志
G02001	西安汽车制动器厂	1	陈六	3	陕西省西安市环城西路北段 127 号	710082	chenl@tom.com	(029)4264666	(029)4264666	1	0
G02002	重庆新工汽配厂	2	张三	2	重庆市大渡口区钢铁路 66 号	400081	zhangs@tom.com	(023)68834947	(023)68834947	1	0
G02003	西安汽车修配厂	3	李四	4	陕西省西安市大庆路 3 号	710082	lis@tom.com	(029)3519107	(029)3519107	1	0
G02004	新疆轴承总厂	2	王五	9	新疆乌鲁木齐市北京北路 42 号	830011	wangw@tom.com	(0991)3716017	(0991)3716017	1	0
G02005	青海汽车配件厂	1	赵六	8	青海省西宁市城东区大众街 69 号	810007	zhaol@tom.com	(0971)8177629	(0971)8177629	1	0

由以上分析可以看出，要集成这两个数据源，不是简单的合并。因此，联网审计环境下的多数据源集成问题应当引起我们的重视。

3.6.2　联网审计环境下面临的主要多数据源集成问题

一般来说，在信息化建设中多数据源集成可以分成三种情况：第一种情况是指把各个