联网审计中的审计预警技术探析

王振莉

（响水县教育局，江苏 响水　224600）

摘　要：联网审计是一种新的审计模式，审计预警是其中的一个重要功能。针对我国联网审计的特点，本文建立了审计预警模型并分析了其关键技术——规则库和不完整数据的检测方法。该模型具有诸多优点。研究结果为我国开展联网审计提供了理论依据。

关键词：持续审计；联网审计；审计预警；审计规则；IT 审计；计算机审计

中图分类号：F239.1；TP399　**文献标识码**：A　**文章编号**：1672－8750(2011)04－0063－04　**收稿日期**：2011－05－30

作者简介：王振莉(1976—　)，女，江苏响水人，响水县教育局会计师，主要研究方向为行政事业会计与审计。

一、引言

持续审计是目前国内外审计领域研究的一个热点问题[1-4]。根据持续审计的研究现状，陈伟等人对持续审计的研究情况进行了分析和总结，认为关于持续审计的研究主要集中在技术实现方法上。根据实现技术方法的不同，他们把持续审计分成嵌入式和分离式两种。分离式持续审计是目前研究的主流，它是指审计模块没有嵌入被审计单位的信息系统中[5]。

我国为了适应计算机审计的需要，已经成功开展了“金审工程”①一期和二期的建设工作，并探索了适合我国国情的持续审计实施方案[5-7]。目前我国正在开展的联网审计也是分离式持续审计的一种方式，其原理如图 1 所示[6-7]。它通过网络采集被审计单位的电子数据，然后进行连续、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，从而使审计工作实现网络化、远程化。它在技术实现上主要包括数据采集与转换、数据传输、数据存储、数据处理等。联网审计的数据采集是通过在被审计单位信息系统端放置一台审计数据采集前置机来实现的。一般来说，审计数据采集前置机的应用系统构架包括数据采集与转换、审计预警、数据发送、采集转换预警规则的控制等几个部分，解决对被审计单位信息系统的数据采集与转换、审计预审和结果报告、数据发送、采集转换预警规则控制等问题。其中，审计预警是一个重要的功能。

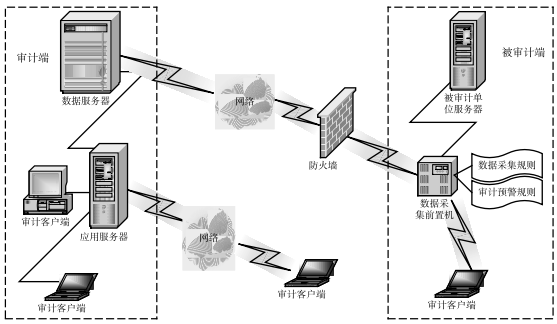

图 1　联网审计原理

我国目前正在大力开展联网审计项目的应用，如财政联网审计项目、地税联网审计项目、海关联网审计项目等，因此，研究联网审计数据采集过程中的审计预警方法对实施联网审计具有重要的理论和实践价值。

二、审计预警模型的原理

联网审计中的审计预警是一个定时触发的审计预查系统，它被部署在被审计单位端的审计数

①“金审工程”是审计信息化的简称，是我国电子政务建设的重大业务系统建设工程，它也是我国“十五”期间首先启动的十二个“金”字号电子政务重大工程之一。

据采集服务器中，该服务器被称为审计数据采集前置机。审计预警模型包括审计预审系统和预审结果报告系统两部分。在联网审计数据采集系统把被审计单位的财务和业务数据采集到审计前置机（托管服务器）的过程中，系统自动启动审计预审系统，利用审计专家系统提供的计算机审计分析指标和可执行方法（预警规则）进行数据分析过滤，把有问题的数据筛选出来。在审计预审系统执行完毕后，审计告警系统自动启动，告知审计人员本次发现的有问题的数据，便于审计人员进行职业分析判断和进一步的延伸审计。

另外，审计预警模型除了需要把不符合业务规则的数据预审出来之外，还需要检测被审计数据中不完整数据的情况，以便审计人员进行决策。因此，检测所采集数据的完整性也是审计预警的一个重要功能。

审计预警主要包括审计预审和预审结果报告两个功能。审计预审功能是系统对采集转换后的审计账表数据按照预先设置的预警规则和计算机审计方法进行批量自动审核分析，将发现的审计疑点存于审计疑点数据库中。预审结果报告则是系统将审计疑点和更改疑点的数据存放到预审结果报告数据库中，并向审计人员发出预审结果报告。

根据以上分析，本文把业务规则和不完整数据检测应用于审计预警之中，提出一种用于联网审计的审计预警方法，如图 2 所示，其原理如下。

1. 根据对被审计单位的业务及数据库系统的分析，在规则库定义相应的业务规则。

2. 根据预定义的数据采集规则，把被审计数据采集到前置机中。

3. 启动基于业务规则的审计预警。在审计预警过程中，对于采集的每条记录，规则库检索模块检索库中的审计业务规则，并据此对每条记录进行检测，内容包括：根据字段的域值来检测一条数据的每个字段；根据同一数据中字段之间的关联关系来进行检测，比如采取函数依赖关系等对每条数据的多个字段进行关联检测。通过以上过程可以判定每条记录是否符合所定义的业务规则，如果记录不符合所定义的业务规则，则将该记录导入前置机系统中的异常数据库。

4. 启动不完整数据检测。根据定义的不完整数据检测方法，系统对采集来的数据进行检测，并把检测出的不完整数据导入前置机系统中的异常数据库。

5. 异常数据库中的异常数据可以存放在前置机系统中，也可以通过网络传输到审计单位，审计人员可以实时或定期地对这些异常数据进行现场或非现场审查。

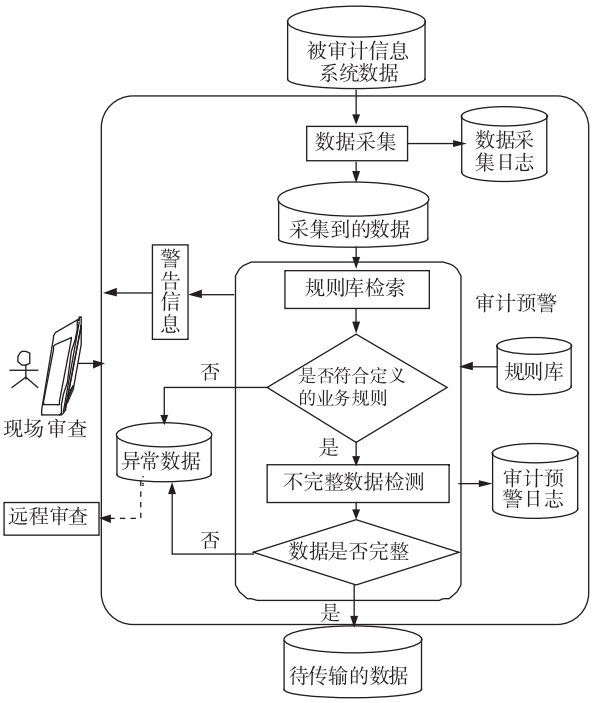

图 2　审计预警模型

三、审计预警模型的关键技术分析

（一）规则库

从图 2 我们可以看出，规则库是审计预警模型的核心。规则库用来存放用于审计预警的业务规则和不完整数据检测规则，主要包括八个方面。

第一，业务规则。业务规则是指符合被审计单位业务的某一数值范围，一个有效数值的集合，或者是指某一种数据模式。业务规则根据其规则内容，可分成通用业务规则和特殊业务规则[6]。

第二，不完整识别规则。它用来指定一条记录为不完整数据的条件，比如记录中字段值缺失比率的阈值。

第三，警告规则。它指定对一些特殊事件的处理规则及相应的提示信息。

第四，审计预警时间控制规则。它用来设置预警触发时间和预警终止时间。

第五，基于业务规则审计控制规则。系统接收到“预警触发”指令后，启动“基于业务规则审

计”功能,利用设置的业务规则,对采集来的审计数据进行审计分析,把筛选出的审计疑点数据列入审计疑点库,并发出“基于业务规则审计”完成指令。

第六,不完整数据检测控制规则。系统接收到“基于业务规则审计”指令后,启动“不完整数据检测”功能,对采集来的审计数据进行自动检测,把检测出的不完整数据导入前置机系统中的异常数据库,并发出“不完整数据检测”完成指令。

第七,审计预审结果报告控制规则。系统接收到“不完整数据检测”指令后,把本次审计预审结果(包括更改疑点库、审计疑点库)形成审计预审结果报告,启动预警终止指令。

第八,数据传输设置控制规则。其功能是接收到审计单位数据中心“接收数据”的指令后启动数据发送功能,把前置机中的数据通过网络传输到审计单位数据中心。

规则语言一般可采用 IF - THEN 规则来完成,其方法如下。

Rule #: IF (< CONDITION1 > AND (OR) < CONDITION2 > AND (OR) …… < CONDITIONn >) is ACTIVED

THEN

(< ACTION 1 > AND (OR) < ACTION 2 > AND (OR) …… < ACTION n >)

END IF

在以上规则中,当达到所设定的条件 < CONDITION > 时,就会触发相应的动作 < ACTION > 。其中,“Rule #”表示规则号;“IF”、“THEN”、“END IF”、“AND”、“OR”均为关键字;“AND”表示它所联系的条件 < CONDITION1 > , < CONDITION2 > …… < CONDITIONn > 必须同时满足,即为“与”的组合;“OR”表示它所联系的条件 < CONDITION1 > , < CONDITION2 > …… < CONDITIONn > 必须有一个满足,即为“或”的组合。

定义审计预警规则的实例如下。

1. 确定性业务规则

Rule 1:IF R_i(实纳税额) <0 Then

该数据为负纳税数据 and 向审计人员发送的警告信息;

END IF;

其中,R_i(实纳税额)表示记录 R_i 中“实纳税额”字段的值。规则 Rule 1 表示如果记录 R_i 中“实纳税额”字段的值小于 0,则该数值为错误数据(负纳税数据)。

在实际应用中,我们可以根据具体的业务特点,在规则库中定义相应的审计预警规则或者修改已有的审计预警规则,从而使该审计预警系统适应不同行业的需要,使之具有较强的通用性和适应性。

(二) 不完整数据的检测方法

审计预警模型除了需要把不符合业务规则的数据预审出来之外,还需要检测被审计数据中不完整数据的情况,以便审计人员进行决策。我们采用陈伟等人提出的方法[7],其原理如下所示。

检测一条记录的不完整程度,是通过计算其缺失字段值的百分比来实现的,方法如下:

假设一条记录可表示为

$$R = \{a_1, a_2, \cdots, a_n\} \quad (1)$$

如果

$$RQ = \frac{m}{n} < r, r \in [0,1] \quad (2)$$

则表示该记录比较完整。

其中,$a_1, a_2, \cdots, a_n$ 表示记录 R 的 n 个字段,m 表示记录 R 中字段值缺失的数目,RQ 表示记录 R 中字段值缺失的比率,r 为记录 R 中字段值缺失比率的阈值。

根据以上分析,不完整数据检测的伪码描述为:

(1) 选取阈值 r,初始化 m 为 0,即 $m=0$;

(2) FOR $i=1$ TO T;//T 为数据表中记录的总数

(3) FOR $j=1$ TO n;

1) IF $R_i(a_j)$ is NULL Then

$m=m+1$

2) END IF;

3) IF $m=0$ Then

直接导入;

4) ELSE

计算 RQ;

5) END IF;

6) IF $QR<r$ Then

该记录标识为不完整数据;

7) END IF;

(4) END;

(5) END;

四、联网审计预警模型的优点分析

通过前文的分析,我们可以看出本文所提出的联网审计预警模型具有很多优点。

1. 本文提出的联网审计预警模型对实现审计工作的三个转变具有重要的参考意义:通过采用审计预警模型,可以实现动态审计;通过采用审计预警模型,可以实现“事中审计”和“事前审计”;通过采用审计预警模型,可以实现对被审计单位的远程监控,从而达到远程审计的目的。

2. 本文设计的审计预警模型类似于嵌入审计模块技术。嵌入审计模块技术是指在一个应用系统中长久嵌入一个审计模块,该模块能检查输入系统中的每一笔事务数据并识别出其中不符合预定义规则的事务数据,审计人员可以对这些识别出的不符合预定义规则的事务数据进行实时的或定期的审查。嵌入审计模块技术是一种有效的计算机辅助审计技术,而本文所设计的审计预警模型不但吸取了嵌入审计模块技术的优点,而且还考虑了我国联网审计的特点和现状,因而更能有效地满足开展联网审计的需要。

3. 使用嵌入审计模块技术需要在被审计信息系统开发时就有所考虑,且需要随着被审计信息系统的升级而进行大幅度修改,而本文所设计的审计预警模型则不需在被审计信息系统开发时就加以考虑,并且和被审计的信息系统相对独立,因此,被审计信息系统升级时,对审计预警模型的影响不大。

4. 传统审计模式下,审计报告需在事件发生几个月甚至半年之后才能生成,采用审计预警模型可以提高审计频率,实现实时持续审计,从而提高了审计报告的价值,降低了审计风险。

5. 采用审计预警模型可以把一些可疑问题提前通知审计人员,审计人员可以远程分析这些可疑问题,然后再根据需要决定是否去现场审计,从而节约了审计经费和审计时间。

当然,采用审计预警模型会增加审计项目前期投资成本,所以在采用审计预警模型时,一定要根据被审计单位的实际情况和实际需要进行,不能盲目上马。

参考文献:

[1] Rezaee Z, Sharbatoghlie A, Elam R, etc. Continuous auditing: building automated auditing capability [J]. Auditing: A Journal of Practice and Theory, 2002, 21: 147 - 163.

[2] Flowerday S, Solms R V. Continuous auditing: verifying information integrity and providing assurances for financial reports [J]. Computer Fraud & Security, 2005: 12 - 16.

[3] 陈伟,尹平. 基于成本效益视角的联网审计可行性分析[J]. 审计与经济研究,2007(1):36 - 39.

[4] 陈伟. 一种基于 AHP 的联网审计绩效评价方法[J]. 审计与经济研究,2011(5):47 - 52.

[5] 陈伟, Qiu Robin, 刘思峰. 持续审计(CA)研究综述[J]. 小型微型计算机系统,2008 (9):1755 - 1760.

[6] 曹洪泽,刘强. 联网审计及其关键技术研究[J]. 北京理工大学学报,2006 (7):614 - 617.

[7] 国家 863 计划审计署课题组. 计算机审计数据采集与处理技术研究报告[M]. 北京:清华大学出版社,2006.

[8] 陈伟,陈耿,朱文明,等. 基于业务规则的错误数据清理方法[J]. 计算机工程与应用,2005(14):172 - 174.

[9] 陈伟,丁秋林. 数据清理中不完整数据的清理方法[J]. 微型机与应用,2005(2):44 - 55.

(**责任编辑:**黄　燕)

Study on Audit Alerts in Online Auditing

WANG Zhen-Li

Abstract: Online auditing is a new mode with audit alerts an important part of this system. Based on the characteristics of online auditing in China, this paper established an audit alert model and analyzed its key technologies, namely, the rule base and detection method for incomplete data. This study may provide theoretical evidence for our online auditing.

Key words: continuous auditing; online auditing; audit alerts; audit rules; IT audit; computer-aided audit