第 3 章　信息系统审计方法与工具

信息系统审计方法与工具是审计人员为了完成信息系统审计任务所采取的各种手段。在信息系统审计工作中，要完成每一项审计工作，都应选择合适的审计方法与工具。本章首先介绍初步审查信息系统的方法和计算机辅助审计技术，对其适用性和优缺点进行了分析和比较，然后重点介绍了数据库查询工具 SQL 和其他审计技术工具。

3.1　信息系统初步审查的技术方法

3.1.1　访谈法

访谈法是指审计人员通过面对面，或者在线视频、音频等方式与被审计单位相关人员交谈，以了解被审计对象的信息。在信息系统审计中，通过与被审计单位的高层管理人员、信息部门管理人员、各业务部门的信息系统使用人员和内部审计人员访谈和交流，主要了解信息系统规划、实施、应用与管理控制等方面的情况。常见的访谈内容及对象如表 3-1 所示。

表 3-1　访谈法的内容和被访问的对象

询问的问题	被访问的对象
了解信息系统的概况，包括主要子系统及基本功能	信息部门主管
了解原始数据来源与数据流向	数据管理员
了解是否有内部控制措施以限制对信息系统和数据的接触	信息部门主管、系统管理人员
了解组织内部控制措施从经济上来看是否合理	高层管理人员、信息部门主管
如果在应用系统中发现错误，了解错误性质并跟踪起因	高层管理人员、信息部门主管、内部审计人员
了解重要的(或重大的)错误是否能得到及时、恰当地纠正	高层管理人员、信息部门主管
了解信息系统的运行情况和满意度	系统操作人员
了解信息系统如何影响系统用户的工作质量	应用系统使用人员
了解信息系统对组织的影响情况	高层管理人员、信息部门主管

审计访谈按照访谈过程的控制程度划分为结构性访谈和非结构性访谈。结构性访谈需要事先设计、精心策划，有调查表或问题清单等书面资料，信息系统审计人员对访谈过程实施有力的控制，常用于完成调查表或流程图。非结构性访谈无须事先策划，过程自由，没有过多控制，常用于审计初步调查。

审计访谈按照参加人数划分为个别访谈和会议访谈。个别访谈是内部审计人员和被访者一对一的面谈，会议访谈是内部审计人员和被访者的一方或双方有多人参加的访谈。

审计访谈和书面沟通方式相比有如下优点：可以直接得到反馈，可以就复杂问题做充分调查，可以得到更多细节，可以短时间内反复交流，有利于建立与客户的友好关系。

审计访谈的缺点可能有以下几个：口头信息不能直接形成审计证据，口头信息不如书面信息严谨，口头表达错误没有机会更改。

尽管如此，这些缺点并不妨碍访谈成为重要的数据收集途径。

3.1.2 问卷调查法

问卷调查法是通过书面或口头回答问题的方式收集研究对象的相关资料，并做出分析综合，得到某一结论的研究方法。

问卷调查法是审计调查中较为广泛使用的一种方法。问卷调查法是在制定调研计划的基础上，通过问卷的形式来了解被审计单位的基本情况、信息系统开发与实施情况。问卷调查法的质量高低关键在于调查表的设计、问题的性质、提问的技巧、度量的尺度、调查表的布局都是重点要考虑的因素。一般而言，设计问卷有以下 6 种形式。

(1) 自由叙述式。不给被调查者提供任何答案让其按自己的思想用文字自由地回答。

(2) 多重选择式。让被调查者从提供的互不矛盾的答案中选择出一个或几个答案来。

(3) 判断式。让被调查者以“是”或“否”二选一的方法回答。

(4) 评定量表法。让被调查者按规定的一个标准尺度对提供的答案进行评价。

(5) 确定顺序式。让被调查者对提供的几种答案按一定的标准(好恶或赞同与否等)做出顺序排列。

(6) 对偶比较式。把调查项目组成两个一组让被调查者按一定的标准进行比较。

这六种问卷类型各有其优点和缺点，审计人员要根据审计目标和任务等，综合运用这几种形式，精心设计调查问卷。设计调查表时，要考虑以下 3 方面的因素。

(1) 问卷调查对象的特性。设计的问题要考虑回答者的专业水平，如果回答者是信息部门主管、系统管理员或企业内部审计人员，则可以提问一些专业性的问题，提问时可以使用计算机方面的专业术语；如果回答者是信息系统的普通用户，则只能提问一些业务应用层面的问题，提问时如果使用专业术语，则需要对专业术语进行解释。

(2) 需要收集的信息内容及其属性。应设计一些事实性的问题，以便回答者能正确理解审计人员的目的所在。

(3) 问卷的管理方式。即问卷的发放方式、回收方式、汇总方式等。

调查问卷法的优点首先是调查结果容易量化，审计人员可以全面地了解被审计单位环境及其信息系统，相对于其他审计方法节省时间、经费和人力，易于实现。其次是可以针对性地了解审计人员关注的信息系统风险点，有利于后续审计工作的推进和深入。

问卷调查法的缺点是对于不同行业、不同规模和信息化水平不同的单位，标准问题的调查问卷会显得不太适用，对于每个被审计系统，审计人员必须有针对性地设计调查问卷，这将是一项繁重的任务。

3.1.3 检查法

检查法是指信息系统审计人员对组织内部或外部生成的记录和文件(包括但不限于纸质、电子或其他介质形式存在的资料)进行检查，或对资产进行实物检查。

查阅软件文档是了解被审计单位信息系统最重要的手段之一。软件文档是用来记录、描述、展示软件项目开发过程中一系列信息的处理过程，通过书面或图示的形式对软件项目整体活动过程或结果进行描述、定义、规定、报告及认证。信息系统审计人员审阅可行性研究报告、系统分析说明书、现状分析报告、输入输出和代码调查表等文档，检查上述文档以及

相应的信息系统建设、应用、管理、运行是否符合国家法律法规、行业标准以及组织内部规章制度等。

根据查阅目的不同，查阅法又可以细分为审阅法、核对法、分析法和比较法等几种形式。审阅法是对被审计组织的信息系统的文档资料以及被审单位的会计资料和其他资料进行详细阅读和审查的一种审计方法。审阅法侧重于包括软件文档在内的书面资料的真实性、合法性。审阅法是最基本、最重要的方法。核对法是指核对被审计组织的信息系统处理流程与相关软件文档内容等的一致性、系统处理流程与业务处理流程的一致性、系统操作执行与内部控制规定的一致性等，以获取审计证据的方法。可以采用软件测试手段核对信息系统实际处理流程与技术文档之间的一致性。分析法是对被审计组织的信息系统流程的分析，目前业务流程的分析，采用数据流图、控制流程图等技术进行分析，通过分析了解被审单位的管理情况、内部控制情况、信息系统运行情况等。比较法通过信息系统输入与输出的比较、信息系统应用与实际结果的比较，以及与同行业其他企业信息系统投入与功能等方面的比较，以证实某个审计事项的真实性和可靠性，获得审计证据的一种方法。在实际工作中，应当灵活运用这些方法，才能收到比较好的效果。

在进行信息系统审计时，要根据审计的目标，查阅相关的文档。如果要对被审计单位的内部控制制度进行审计测试，则可以查阅以下信息系统内部控制和管理的文档。

(1) 被审计单位的职责说明书或程序手册。

(2) 被审计单位的组织结构图，特别是 IT 部门的组织结构及职责分工。

(3) 有关信息系统的管理决策与规划资料。

(4) 信息系统规划、开发、实施、应用与管理文件。

(5) 与信息系统有关的会议记录。

(6) 信息系统操作手册。

(7) 系统评审会记录与系统维护。

(8) 日志文件。

(9) 信息系统管理制度与灾难恢复计划。

(10) 前任审计的工作底稿。

通过内部控制文档资料层面的测试，可以形成控制测试表。以下以查阅公司的职责说明书和组织结构图初步形成组织管理的控制测试矩阵为例来说明(表 3-2)。

表 3-2　组织管理的控制测试矩阵

序号	控制措施	控制目标		备注
		职责分离	人员管理控制	
1	是否制定了职责分离的规章制度	√	√	
2	业务人员的工作职责明确清晰	√	√	
3	信息技术部门只负责信息系统的开发和维护工作，日常的业务操作只能由相关业务部门的工作人员来进行	√		
4	信息技术人员未经批准不能接触备份的数据，不能在无监督的情况下进行数据备份和恢复的工作	√		
5	系统的输入人员与复核人员不能相互兼任	√		
6	操作人员不能保管除操作手册以外的系统技术文档	√		

续表

序号	控制措施	控制目标		备注
		职责分离	人员管理控制	
7	业务操作人员不能管理系统产生的重要的业务档案	√		
8	聘用人员与工作岗位是否相符		√	
9	对接触秘密数据的工作人员签订保密协议书		√	
10	对关键性业务配备了后备人员		√	
11	定期对工作人员的工作进行考核		√	
12	定期对信息系统人员进行培训		√	
13	关键技术有多人掌握		√	
14	人员离岗后,信息系统中的账号和口令及时删除		√	
15	人员离岗后,及时归还所有的报告、文档和书籍		√	

3.1.4 观察法

观察法是指审计人员到被审计单位的经营场所及其他有关场所进行实地察看,以证实审计事项的一种方法。审计人员运用观察法,观察被审计组织员工的职责履行情况以及业务操作程序等以识别员工的逻辑访问权限是否合规,软硬件物理控制是否有效,盘点信息资产是否安全。实地观察时要求尽可能接近事件发生地去研究真实系统,作为观察者要遵守一定的规则,在观察时尽可能多听,少说或不说,尤其是要注意那些一闪即逝的有用的信息。通过观察业务操作流程和岗位之间相互制约程度以及检查内部制度的执行情况等手段,发现线索并直接获取证据。

观察内容包括被审计单位的经营场所、被审计单位计算机环境下的业务活动和内部控制运行情况、信息系统的物理场所、计算机设施、计算机操作过程、数据备份与存储过程、网络环境下数据库管理的操作过程等。

实地观察法有利于审计人员掌握被审单位和系统的第一手资料,但这种方法也有它的局限。实地观察法的局限是:观察提供的审计证据仅限于观察发生的时间和地点,并且在相关人员已知被观察时,相关人员从事活动或执行程序可能与日常的做法不同,从而影响内部审计人员对真实情况的了解。

3.1.5 风险评估法

风险评估法是指审计人员通过找出被审计单位的信息系统面临的风险及其影响,以及目前安全水平与被审计单位安全需求之间的差距,进而评价被审计单位信息系统风险状况的审计方法。审计人员在实施信息系统审计时,必须评估存在的不同的审计风险,并且选择高风险的区域进行重点审计。在风险评估时可以选择多种风险分析技术,可采用计算机辅助分析,也可以采用人工分析。风险分析的标准可以是简单的定性分类,也可以通过复杂的科学计算进行定量计算。

风险评估常用方法有以下几种。①定性分级技术:根据审计对象的技术复杂性、现有控制程序的水平、可能造成的财务损失等各种因素的风险值累计为总风险值,根据分值大小进行排列分为高、中、低级风险。②经验判断法:审计人员根据专业经验、业务知识、管理

层的指导、业务目标、环境因素等进行判断，以决定风险大小。

按照固有风险、控制风险和检查风险的审计风险理论，对信息系统的设计与建设、运行与维护、检查与监督等各环节的风险进行评估，对各部门的责任进行界定。

根据审计风险理论，任何风险都是多因素集合作用的结果，审计风险也不例外，审计风险由固有风险、控制风险和检查风险三个要素构成。固有风险是指在没有任何相关的内部控制的情况下，某一账户或交易类别单独或连同其他账户、交易类别产生重大错报、漏报的可能性。控制风险是指被审计单位的信息系统内部控制结构政策或程序未能及时防止或觉察重大错误的可能性。检查风险是指内部控制未能察觉并纠正财务报表中的重大错误，运用审计程序也未能发现这些错误的可能性。

3.2　计算机辅助审计技术

在高度计算机化的信息系统中，只采用常规审计方法显然是不够的，无论是审计证据的收集、评价，还是实现审计工作的自动化，都需要借助计算机这个现代化工具才能更高效率地完成。

早在 20 世纪 80 年代，国际会计师联合会在其发布的《国际审计准则 16——计算机辅助审计技术》(1984 年)中就指出："审计程序的运用，可能要求审计人员考虑利用计算机技术作为一项审计的工具。计算机在这方面的各种使用称为计算机辅助审计技术。"

计算机辅助审计技术(Computer Assisted Audit Techniques，CAATs)由于通常使用众多的计算机工具，故通常也被称为计算机辅助审计工具与技术(Computer Assisted Audit Tool and Techniques，CAATTs)。通常情况下，无论信息系统是大型还是小型，是联网还是未联网，审计人员都可以采用计算机辅助审计技术。

计算机辅助审计技术的特点如下。

(1) 在系统中嵌入特殊的审计模块，收集、处理和打印审计证据。

(2) 利用测试数据对信息系统进行评价。

(3) 选择若干事务输入到信息系统中进行处理。

(4) 对运行中的信息系统的变化状态进行跟踪和映像。

(5) 某些情况下，用审计记录保存审计证据，以便今后实施审计。这些记录可以存放在应用系统文件或某个独立的审计文件中。

经过多年的信息系统审计实践，国内外出现了许多计算辅助审计技术。在众多的计算机辅助审计技术中，应用最广泛的是数据测试分析方法，按照是否处理实际业务数据来分，可以分为处理虚拟数据的程序测试方法和处理实际业务数据的程序测试方法两类。

处理虚拟数据的程序测试方法，特点是通过处理事先设计的测试数据来确定应用程序的可靠性。通过设计少量测试数据，对局部或大部分应用程序进行测试，也可根据需要对某特定控制措施进行测试。测试过程：①设计测试数据；②手工处理设计好的数据；③用被测试程序处理已设计好的数据；④比较上述两种方式处理的结果，并推断应用控制的可靠性。具体方法包括检测数据法与整体检测法。

处理实际数据的程序测试方法的特点是使用用户单位的计算机程序处理实际数据以确

定应用控制可靠性。审计人员可以利用已形成的实际数据，无须再设计测试数据，而且用程序处理的结果能表明程序控制的强弱。具体方法包括受控处理、受控再处理法、平行模拟法、嵌入审计程序法、程序追踪法（标记追踪法）。

3.2.1 检测数据法

检测数据法，是指审计人员把一批预先设计好的检测数据，利用被审程序加以处理，并把处理的结果与预期的结果做比较，以确定被审程序的控制与处理功能是否恰当、有效的一种方法。这种方法的工作原理见图 3-1。

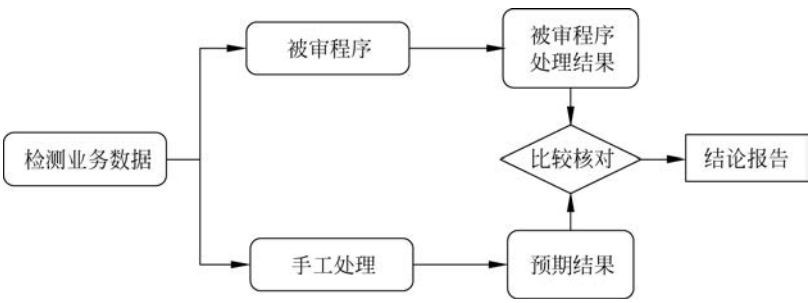

图 3-1 检测数据法的工作原理

检测数据法可用来审查信息系统的全部程序，也可用来审查个别程序，还可以用来审查某个程序中的某个或某几个控制措施，以确定这些控制是否能发挥有效功能。检测数据法一般适用于下列三种情况。

（1）被审信息系统的关键控制建立在计算机程序中。

（2）被审信息系统的可见审计线索有缺陷，难以由输入直接跟踪到输出。

（3）被审单位信息系统程序较多，用检测数据法比直接用手工方法进行审查更经济，效率更高。

1. 检测数据的来源

应用检测数据法对被审程序的处理和控制功能进行审查，选择或设计合适的检测数据是个关键问题，检测数据按其来源可分为以下几种。

（1）被审单位以往设计的检测数据。任何新的信息系统在正式投入使用之前必须对程序进行测试，这是系统开发过程中的必经步骤之一。因此，在信息系统开发时，被审单位通常会投入大量的时间，设计检测数据，以便发现新编写的程序内隐含的各种错弊。若此类检测数据仍然存在，则审计人员也可加以利用，作为检测数据的一部分。另外，被审单位在修改程序后调试检测经修改的程序所用的模拟检测数据，也可作为审计人员的检测数据。

（2）由审计人员自行设计的检测数据。一般来说，审计人员通常可采用下列几种方式，自行设计检测数据。

① 由审计人员根据被审程序控制及处理功能和主文件，设计若干虚拟的业务，并逐笔制作成模拟检测数据。

② 根据被审计单位以前月份或年度的输入数据，稍加修改后利用。

③ 运用审计软件产生检测数据。审计人员可利用检测数据生成软件获得模拟检测数

据。使用软件产生检测数据，可避免检测数据法的许多缺点。例如，人工设计检测数据费时费力，考虑到所有例外情况也困难。但使用软件产生检测数据，其数量可能相当大。因此，以手工计算预期的结果可能要花费较高的成本。此外，检测数据软件的取得及使用成本可能也较高。

2. 检测数据的业务分类

不管检测数据的来源如何，检测数据中应包括下列两类业务。

(1) 正常的、有效的业务，以确定被审程序对有效数据的处理是否正确。这类检测数据可以是被审单位正在准备处理的数据或过去已处理过的历史数据，也可以是审计人员按要求设计出的正常检测数据。

(2) 不正常的、无效的业务，以确定被审程序能否将这些业务检测出来，拒绝接受，并给出错误信息，以便修改。例如：

① 不合理的业务：业务的有关数值超出了其极限值。

② 无效的业务：科目代码或单位代码等为无效代码的业务。

③ 不完整的业务：空的业务。

④ 顺序错误的业务：要求顺序编号的字段如记账凭证编号等出现缺漏或重复。

⑤ 溢出业务：输入的数据超出该字段预定的宽度等。

对于不正常的、无效的业务，在实际应用时，要根据被审程序的控制功能及具体的审计目的，确定检测数据中不正常业务的类型。对于正常的、有效的业务，审计人员要注意被审程序的功能覆盖问题，即选择的检测数据要能检查到被审程序的所有处理和控制功能。对此，可采用决策表的方法来选择和设计检测数据。

3. 检测数据法的优点

(1) 对审计人员的计算机知识和技能的要求不太高。

(2) 适用范围较广。

(3) 在审计线索间断或不完整的情况下，使用这种方法也能对程序的功能做出评价。

(4) 由于这是一种抽样审计方法，因此，用于测试比较复杂的被审程序是比较经济的。

4. 检测数据法的缺点

(1) 在全面测试被审系统的所有程序或程序中所有控制及处理功能时，难以保证测试数据的全面性，因而难以对被审程序做出全面的评价。

(2) 如果利用被审单位实际运行的程序和文件处理模拟检测数据，还可能破坏被审单位的主文件。

(3) 难以保证被审的程序就是被审单位在整个被审期间实际使用的程序。由于检测数据法只能证明在处理检测数据时被审程序的处理和控制功能是否正常，因此，审计人员所抽查的应用程序，很可能并非被审期间实际应用程序，特别是当被审程序有不同版本时，此种情况很可能发生。因此，使用检测数据法，审计人员必须首先确定被审的程序确为被审期间实际运行的程序。对此，可采取突击审计的方式，在审计人员的监督下，要求被审计单位数据处理部门的人员将机内正在运行的程序复制一份，审计人员用此复制的程序采用检测数据法进行审查。另外，审计人员还应检查系统的一般控制是否健全、有效。例如，被审程序的维护控制以及被审程序的接触控制等是否有效。只有相应的一般控制是健全有效的，审

计人员才能依靠检测数据法的审查结果。

3.2.2 整体检测法

整体检测法，是指审计人员在被审的信息系统中建立一个虚拟的实体（如虚拟的部门、车间、经销商、顾客、职员、账户或其他任何会计信息的累计单位），然后利用被审程序，在正常的业务处理时间里，与真实业务一起，对此虚拟实体建立的有关检测业务由同一被审程序进行处理，并把被审程序对这些检测业务处理的结果与预期的结果进行比较，以确定被审程序的处理和控制功能是否恰当、可靠的方法。

整体检测法的工作原理见图 3-2。

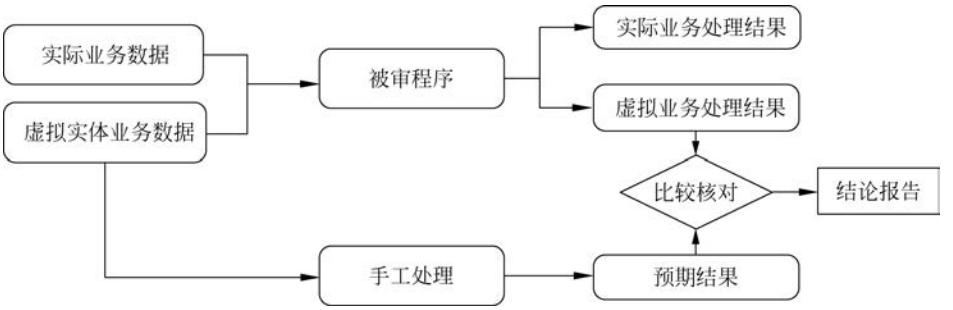

图 3-2 整体检测法的工作原理

采用整体检测法的审计步骤如下。

（1）确定需要审查的程序以及需要审查的处理及控制功能。

（2）虚拟一个实体。

（3）设计与虚拟实体有关的业务，并用手工计算出预期的结果。

（4）将虚拟实体的业务数据与被审计单位的实际业务数据一并输入被审系统，由被审程序进行处理。

（5）将被审程序的处理结果与手工计算的预期结果进行比较，做出评价。

（6）消除虚拟实体的业务数据，以免影响真实数据处理结果的正确性。

例如，现要审查被审计单位的工资处理程序，该程序有这样一个控制措施：若某职工的工资经过处理后，其实发工资额超出 1500 元，则被审程序将该职工工资数据记入到异常数据文件中并打印输出，供会计主管审核。若用整体检测法来测试该程序中的这项控制措施，可以设计一个职工，该职工的职工号码不同于任何一个实际的职工号码，设计一组有关该职工的基本工资、扣款、补贴等数据。假如通过手工计算该职工的实发工资数额为 1650 元，将这组数据输入计算机处理后，若有关数据没有记入到异常数据文件中，也没有打印输出，则说明该程序没有实发工资的合理性检验措施，或者这种控制措施已不起作用。

采用整体检测法，有下列两种常见的使用方式。

（1）让检测业务如真实业务一样从头到尾通过整个系统得到最终的输出。这时，审计人员要在处理至某一阶段或结束以后，准备一些会计分录冲销检测业务，以防影响被审计单位数据文件的正确性。

（2）对被审信息系统的被审程序做适当的修改，以便检测业务在进入总分类账或重要

的输出之前被删除，不致影响被审计单位的正常业务和财务报表。但是，在系统运行以后，修改系统的应用程序成本较高，也很困难。因此，除非在信息系统的开发阶段，审计人员已考虑到要用整体检测法进行审计，而嵌入删除检测业务的审计程序段，否则，这种方式较少采用。

例如，在上述例子中，假设该职工为生产工人，若采用第一种检测方式，则为了消除该虚拟职工对工资分配和总分类账的影响。应准备会计分录：

借：应付工资

贷：生产成本

输入系统进行冲销。若采用第二种检测方式，则可修改工资结算汇总程序和工资分配汇总程序，令其在汇总时对职工号码超过实际职工号码范围的职工单独进行汇总，并单独打印输出，不汇总入实际职工工资数额中。检测完毕后，可令程序从职工工资文件中删除这些业务。

1. 整体检测法的优点

（1）检测数据可与被审计单位日常处理的真实业务一起输入，并进行处理。因此，可能较其他审计方法更为经济有效。

（2）审计人员可根据需要随时输入检测数据，从而能够对被审程序进行经常性的直接测试，保证被审程序就是被审计单位实际运行的程序，保证审计结果的可靠性。

（3）应用范围广泛。它既适用于在线实时系统，也适用于批处理系统。随着在线实时系统的逐渐普及，未来整体检测法的应用必然会比检测数据法更为广泛。

2. 整体检测法的缺点

（1）如果没有及时或完全消除检测数据，可能会影响被审计单位数据文件和财务报表的正确性。因此，审计人员应详细考虑检测数据对系统各种数据文件的影响，冲销业务能否全部冲销这些影响。

（2）由于整体检测法是根据被审程序对检测数据的处理结果来推断程序的处理和控制功能的正确性，因此，它与检测数据法一样，如果检测数据选择不全面，则不能审查出被审程序中的全部错弊。另外，如果被审计单位的数据处理人员知道检测业务，也可能会加以干预，从而影响审计结果。因此，进行整体检测，当检测数据输入计算机时，审计人员应对系统的操作进行适当的监督。

3.2.3　受控处理法

受控处理法，是指审计人员通过被审程序对实际会计业务的处理进行监控，查明被审程序的处理和控制功能是否恰当、有效的方法。采用这种方法，审计人员首先对输入的数据进行查验，并建立审计控制，然后亲自处理或监督处理这些数据，最后将处理的结果与预期结果加以比较分析，判断被审程序的处理与控制功能能否按设计要求起作用。例如，审计人员可通过检查输入错误的更正与重新提交的过程，判断被审程序输入控制的有效性，通过检查错误清单和处理打印结果来判断被审程序处理控制和功能的可靠性，通过核对输出与输入来判断输出控制的可靠性。

下面以审查存货核算程序为例来说明受控处理法的原理。存货业务有两方面，一是存货入库引起存货数量和金额的增加，二是存货发出引起存货数量和金额的减少。在输入这

两方面的数据前，审计人员将它们的总数量、总金额和业务笔数分别予以统计，然后用被审程序输入和处理这些数据，处理完后，将打印的结果与事先算得的存货增加和减少的数量、金额以及业务笔数加以核对，就可以判断被审程序的处理与控制功能的可靠性；如果该系统中事先存放单位所有存货的编码，若输入的存货编码在系统中不存在，则该程序应拒绝输入和处理，若被审程序没有拒绝，照常处理，则说明被审程序对存货编码检验措施不存在或已不起作用，这时审计人员可采用其他的审计方法对被审程序进一步进行审查。

1. 受控处理法的主要优点

受控处理法的主要优点是，审计技术简单，省时省力，不需要审计人员具有较多的计算机知识，只要采取突击审计的方式，就可以保证被审程序与实际使用程序的一致性，从而保证审计结论的可靠性。

2. 受控处理法的主要缺点

（1）选择的实际业务数据可能不足以评价各种处理和控制功能。实际业务数据多为正确数据，要想找到足够的业务数据对被审程序的各种处理和控制功能进行评价往往是不可能的。

（2）要求审计人员具有相当的操作知识与技能，以便对被审程序运行过程进行有效的控制与监督，防止被审计单位操作人员篡改程序或数据。

（3）审计人员对实际业务数据的监督、控制及比较分析，可能会影响被审计单位的正常数据处理及工作效率。

3.2.4 受控再处理法

受控再处理法，是指在被审计单位正常业务处理以外的时间里，由审计人员亲自进行或在审计人员的监督下，把某一批处理过的业务进行再处理，比较两次处理的结果，以确定被审程序有无被非法篡改，被审程序的处理和控制功能是否恰当、有效。运用这种方法的前提是以前对此程序进行过审查，并证实它原来的处理和控制功能是恰当、有效的。因此，这种方法不能用于对被审程序的初次审计。

鉴于受控再处理法的含义，在实际审计工作中，根据情况，可采用下列两种不同方法。

（1）审计人员保存一批在以前审计时已由当时经审查证实处理和控制功能恰当、有效的被审程序处理过的业务及当时处理的结果。审计人员可把这批业务输入被审系统由当前实际运行的被审程序进行处理，得出当前的处理结果，比较两次处理结果，从而确定当前实际运行的被审程序有无改动，处理和控制功能是否可靠。其工作原理见图 3-3。

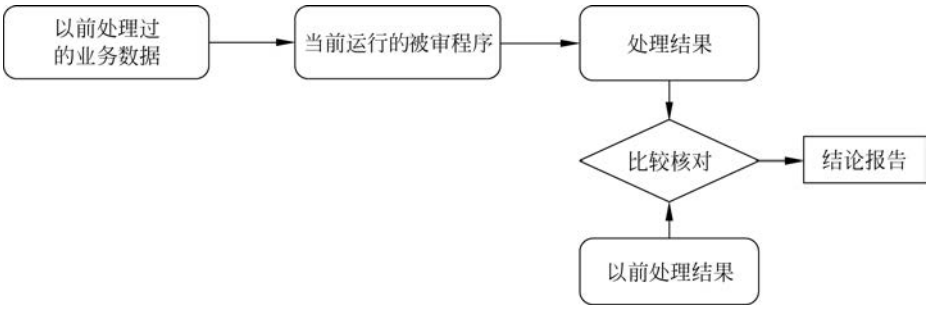

图 3-3 受控再处理法的工作原理（1）

(2) 审计人员保存有以前审计时已经审查证实其处理和控制功能恰当、有效的被审程序副本,审计人员可把当前被审程序处理过的业务输入系统由审计人员保存的被审程序副本进行处理,得出处理结果,比较两次处理结果,从而确定当前实际运行的被审程序有无非法改动。其工作原理见图 3-4。

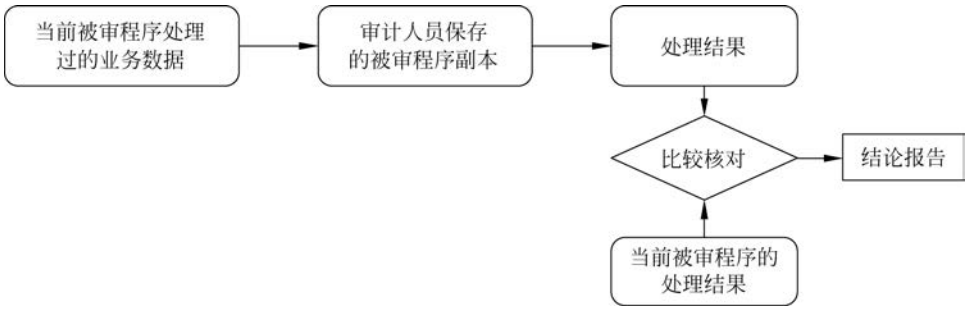

图 3-4　受控再处理法工作原理(2)

受控再处理法的优点是测试数据是现成的,而且可在审计人员和被审单位都感到方便时进行测试。因此并不干扰被审计单位的正常业务。其缺点是,有些单位已经处理过的业务文件可能只保留很短的时间,而主文件可能经过了多次更新。因此难以获得重新处理所需的文件。

3.2.5　平行模拟法

平行模拟法,是指审计人员自己或请计算机专业人员编写的具有和被审程序相同处理和控制功能的模拟程序,用这种程序处理当期的实际数据,并以处理的结果与被审程序的处理结果进行比较,以评价被审程序的处理和控制功能是否可靠的一种方法。这种方法的原理可用图 3-5 表示。

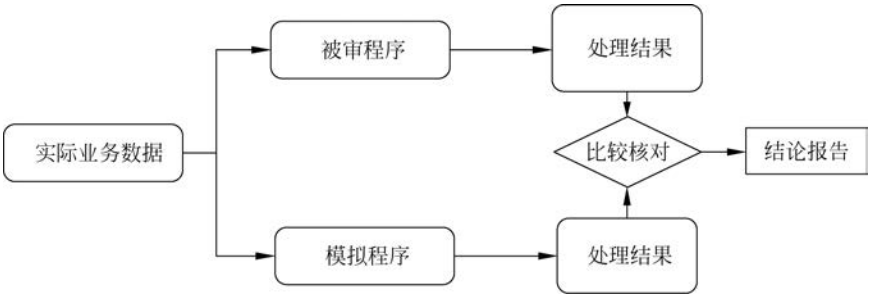

图 3-5　平行模拟法的工作原理

使用这种方法的一般步骤如下。

(1) 根据审计的目的和要求,确定被审程序。

(2) 了解该程序所涉及文件的记录格式、文件类型、数据处理步骤和计算规则,输入输出的格式和内容,输入、处理、输出控制措施等。

(3) 编制审计模拟程序。

(4) 分别用被审程序和模拟程序处理实际业务数据。

(5) 对处理结果进行比较分析,并对被审程序的处理和控制功能做出评价。

运用这种方法,审计人员不一定要模拟被审程序的全部功能,可以只模拟被审程序的某一处理功能或控制功能。这种方法一般可用于工资计算、材料成本差异的计算、产品销售成本的计算以及利润和税金的计算等方面,这些方面计算量大,但有一定的数学模型,因此程序的模拟较为简单。

采用平行模拟法的优点在于,它能独立地处理实际数据,不依赖被审计单位的人力和设备,因而审计结果较为准确。其主要缺点是开发模拟系统难度较大且成本较高,而且对于审计人员来讲,要自己开发一个模拟系统程序是很困难的,如果是简单的模拟程序,则用计算器也能达到相同的效果。因此,这种方法在目前来讲很难做到。另外,审计人员首先要证明模拟程序是正确的,这也是一个额外的困难。

3.2.6 嵌入审计程序法

嵌入审计程序法,是指在被审信息系统的设计和开发阶段,在被审的应用程序中嵌入为执行特定的审计功能而设计的程序段,这些程序段可以用来收集审计人员感兴趣的资料,并且建立一个审计控制文件,用来存储这些资料,审计人员通过这些资料的审核来确定被审程序的处理和控制功能的可靠性。这种方法的原理见图 3-6。

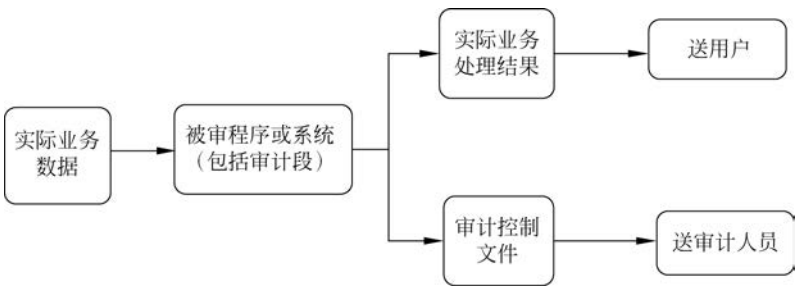

图 3-6 嵌入审计程序法工作原理

在实际应用中,审计程序段主要有两种,一种是不经常起作用的,只有审计人员在执行特定的审计任务时才激活的审计程序。例如,在应收账款核算程序中嵌入的给债务人打印审计函证书的审计程序段,这种审计程序平时不起作用,只有在审计人员要打印审计函证书时才使用。另一种是在被审程序中连续监控某些特定点上处理的程序,当实际业务数据输入被审系统,由被审程序对其进行处理时,审计程序段也对数据进行检查,如果符合某些条件,则将其记入审计控制文件中,审计人员可以定期或不定期地将审计控制文件打印输出,以便对被审程序的处理和控制功能进行评价,或对系统处理的业务进行监控。例如,在现金核算过程中,审计人员要检查被审计单位有无违反现金管理制度,可嵌入审计程序段,该程序段检查每笔现金收付业务是否超出范围和限额,若超出,则把这笔业务记入审计控制文件中。通过检查审计控制文件,可发现被审计单位有无违反现金管理制度的情况。又如,在某单位的工资核算程序中,程序计算出每一个职工的实发工资额后检查该职工的工资额有无超出规定的限额,若超出,将其打印输出,供会计主管审核。审计人员现要审核该工资核算程序对实发工资限额检查是否有效,可在被审程序中插入一段程序,对超出限额的实发工资写入审计控制文件中,定期将审计控制文件打印输出,与被审程序的打印输出结果进行核

对，以查明被审程序该项控制的有效性。

1. 嵌入式审计的优点

（1）审计证据的客观性。由于嵌入的审计模块本身具有隐蔽性，非审计人员难以干涉和更改自动形成的审计数据。所以，审计人员能够通过这些审计模块客观地取得对被审系统测试的结果，形成审计证据。

（2）在被审单位处理业务数据的同时获取审计证据，可保证审计数据真实来自被审单位实际应用系统，可以弥补数据处理后进行的审计测试中难以确信被审程序是否就是被审单位实际应用系统的缺陷。

（3）可以获得实时的审计数据。只要被审程序开始运行，审计程序模块就处于监控状态，可以实现连续搜集充足的审计线索。

2. 嵌入式审计的缺点

（1）会降低信息系统的性能。审计模块与被审程序并行运行，会增加系统的内存占用与开销。

（2）嵌入的审计模块本身可能会存在安全性、完整性问题，会影响被审计系统的正常运行。

（3）要取得被审单位的积极配合存在一定难度。这种方法要求审计人员在系统开发之初就参与系统的分析与设计，完成审计模块的嵌入，然而被审计单位出于隐私保护以及系统安全性的考虑，一般不愿意让审计人员在其应用系统中嵌入审计模块。这种方法更适用于内部审计机构，当使用这种方法时，审计人员还要特别注意被审系统的一般控制是否健全有效，以防审计程序段被有关人员移走或被篡改。

3.2.7　程序追踪法

程序追踪法是一种对给定的业务，跟踪被审程序处理步骤的审查技术。一般可由追踪软件来完成，也可利用某些高级语言或数据库管理系统中的跟踪指令跟踪被审程序的处理。

在手工会计系统中，对于一笔业务，可以从原始凭证跟踪审查到记账凭证、账簿和报表。在信息系统中，这些原来由人工来完成的追踪工作可以由计算机进行。

采用这种方法的优点是，可列示被审程序中什么指令已执行以及按何种顺序执行。因此，追踪法可查出在被审程序中的非法指令。它的缺点是，要求审计人员具有编写应用程序所用的计算机语言的充分知识，实行跟踪并分析结果可能费时费力。因此，这种方法在实际审计工作中应用并不广泛。

本节论述了计算机辅助信息系统应用程序审计的方法，这些方法并不是孤立的，而是相互联系的。在实际审计工作中，审计人员应根据被审计信息系统应用程序的具体情况和自己的计算机知识水平，具体的审计目的、审计时间和经费条件等，合理地选择其中一种或几种审计方法。

3.3　数据库查询工具

结构化查询语言（Structured Query Language，SQL），是一种特殊目的的编程语言，是一种数据库查询和程序设计语言，用于存取数据以及查询、更新和管理关系数据库系统。

SQL 于 1974 年由 Boyce 和 Chamberlin 提出，并首先在 IBM 公司研制的关系数据库系统 System R 上实现。由于它具有功能丰富、使用方便灵活、语言简洁易学等突出的优点，深受计算机工业界和计算机用户的欢迎。目前，绝大多数流行的关系型数据库管理系统，如 Oracle、Sybase、Microsoft SQL Server、Microsoft Access 都支持 SQL 作为查询语言。

SQL 具有数据定义、数据操纵和数据查询的功能。

3.3.1 数据定义

（1）定义基本表。采用 SQL 定义基本表的语法如下：

```
CREATE TABLE 表名[表约束]
列名 1 数据类型[默认值 1,列约束 1]
列名 2 数据类型[默认值 2,列约束 2]
…
列名 n 数据类型[默认值 n,列约束 n];
```

（2）删除基本表。采用 SQL 删除基本表的语法如下：

```
DROP TABLE 表名;
```

（3）修改表。采用 SQL 修改表的语法如下：

```
ALTER TABLE 表名
[ADD <新列名><数据类型>[列级完整性约束条件]]
[DROP <完整性约束条件>]
[ALTER COLUMN <列名><数据类型>];
```

其中，“表名”是要修改的基本表，ADD 子句用于增加新列和新的完整性约束条件，DROP 子句用于删除指定的完整性约束条件，ALTER COLUMN 子句用于修改原有的列定义，包括修改列名和数据类型。

3.3.2 数据操纵

（1）插入数据。插入数据语句语法如下：

```
INSERT INTO 表名[(列名 1,列名 2,…,列名 n)]
VALUES(值 1,值 2,…,值 n);
```

（2）修改数据。对表中已有数据进行修改，语句语法如下：

```
UPDATE 表名
SET 列名 1 = 表达式 1,列名 2 = 表达式 2,…
WHERE 条件;
```

（3）删除数据。删除数据的语句语法如下：

```
DELETE FROM 表名
WHERE 条件;
```

（4）增加列。在已存在的表中增加新列，语句语法如下：

```
ALTER TABLE 表名
```

```
ADD[新列名 数据类型(长度)];
```

(5) 删除表。将已经存在的表删除,语句语法如下:

```
DROP TABLE 表名;
```

3.3.3　数据查询

SQL 提供了 SELECT 语句进行数据库查询,SELECT 语句在审计中应用较为广泛,本节介绍其基本语法及使用。

1. SELECT 语句的基本语法

```
SELECT [ALL |DISTINCT]<目标列表达式>[,<目标列表达式>]…
FROM <表名或视图名>[,<表名或视图名>]…
[WHERE <条件表达式>]
[GROUP BY <列名 1 >[ HAVING <条件表达式>]]
[ORDER BY <列名 2 >[ASC |DESC]];
```

下面以某市“出租车补贴数据”为例,来介绍 SQL 语句的使用,“出租车补贴数据”表结构(部分字段)如图 3-7 所示。

	A	B	C	D	M	N	O	P	Q	R	S	T	U	V	W
1	单位名称	车牌号码	车牌颜色	营运证号	实际运营天数	日均载客次数	日均载客里程	日均运营里程	年初千米数	年末千米数	全年行驶里程	全年汽油消耗总量	百千米平均单耗汽油	补贴标准	补贴金额
2	出租车个体	江K62711	蓝色	331515300044	212	32	185	222.22	0	47111	47111	3770	8	1.1915	4491.955
3	出租车个体	江K7T303	蓝色	331515301013	204	32	185	222.22	0	45333	45333	3626	8	1.1915	4320.379
4	出租车个体	江K6T418	蓝色	88551963	204	32	185	222.22	0	45333	45333	3626	8	1.1915	4320.379
5	A公司	江K6T442	黄色	331515300933	204	32	185	222.22	0	45333	45333	3626	8	1.1915	4320.379
6	A公司	江K6B475	黄色	331515301464	204	32	185	222.22	0	45333	45333	3626	8	1.1915	4320.379
7	A公司	江K6T293	黄色	331515300408	158	32	185	222.22	0	35110	35110	2810	8	1.1915	3348.115
8	A公司	江K6B050	黄色	331515301516	202	32	185	240	0	48480	48480	3877	8	1.1915	4619.4455
9	A公司	江K6T448	黄色	88552034	202	32	185	240	0	48480	48480	3877	8	1.1915	4619.4455
10	B公司	江K6T460	红色	331515300551	202	32	185	240	0	48480	48480	3877	8	1.1915	4619.4455
11	B公司	江K6T402	红色	331515300901	202	32	185	240	0	48480	48480	3877	8	1.1915	4619.4455
12	B公司	江K6T537	红色	331515300185	103	32	185	222.22	0	22889	22889	1830	8	1.1915	2180.445
13	B公司	江K6T168	红色	331515300187	103	32	185	222.22	0	22889	22889	1830	8	1.1915	2180.445
14	B公司	江K6T149	红色	331515300191	103	32	185	222.22	0	22889	22889	1830	8	1.1915	2180.445
15	B公司	江K6T527	红色	331515300192	103	32	185	222.22	0	22889	22889	1830	8	1.1915	2180.445
16	B公司	江K6T443	红色	331515300953	203	32	185	222.22	0	45110	45110	3610	8	1.1915	4301.315
17	C公司	江K6T598	蓝色	331515300151	104	32	185	240	0	24960	24960	1996	8	1.1915	2378.234
18	C公司	江K6B935	蓝色	331515301351	203	32	185	222.22	0	45110	45110	3610	8	1.1915	4301.315
19	C公司	江K62053	蓝色	331515301487	202	32	185	240	0	48480	48480	3877	8	1.1915	4619.4455
20	C公司	江K6B357	蓝色	331515300958	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
21	C公司	江K6T318	蓝色	331515300960	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
22	C公司	江K6B086	蓝色	331515301441	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
23	C公司	江K62710	蓝色	331515300661	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
24	C公司	江K6T571	蓝色	331515300163	104	32	185	222.22	0	23111	23111	1850	8	1.1915	2204.275
25	C公司	江K6T572	蓝色	331515300164	104	32	185	222.22	0	23111	23111	1850	8	1.1915	2204.275
26	D公司	江K60179	蓝色	331515300166	104	32	185	240	0	24960	24960	1997	8	1.1915	2379.4255
27	D公司	江K6T240	蓝色	331515300462	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
28	D公司	江K6T393	蓝色	331515300556	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
29	D公司	江K6T242	蓝色	331515300920	239	32	185	222.22	0	53110	53110	4250	8	1.1915	5063.875
30	D公司	江K6T257	蓝色	88551924	238	32	185	222.22	0	52888	52888	4233	8	1.1915	5043.6195
31	D公司	江K7T366	蓝色	331515301196	235	32	185	222.22	0	52222	52222	4177	8	1.1915	4976.8955
32	D公司	江K6T841	蓝色	88551934	235	32	185	222.22	0	52222	52222	4177	8	1.1915	4976.8955

图 3-7　“出租车补贴数据”表结构(部分字段)

2. 单表查询

1) 选择表中的若干列

(1) 查询指定列。SQL 语句中要注意:“,”“;”等符号必须要在英文状态下输入,否则不能正确执行。

① 查询“出租车补贴数据”中所有的车牌号码与营运证号。

```
SELECT 车牌号码,营运证号
```

```
FROM 出租车补贴数据;
```

② 查询“出租车补贴数据”中所有的车牌号码、营运证号、实际运营天数、全年行驶里程。

```
SELECT  车牌号码,营运证号,实际运营天数,全年行驶里程
FROM 出租车补贴数据;
```

(2) 查询全部列。将表中的所有属性列都选出来,有两种方法:在 SELECT 关键字后面列出所有列名;如果列的显示顺序与其在被查询表中的顺序相同,可将<目标列表达式>指定为“*”。

查询“出租车补贴数据”中所有的记录。

```
SELECT   *
FROM 出租车补贴数据;
```

(3) 查询经过计算的值。

查询“出租车补贴数据”中车牌号码以及年末千米数与年初千米数的差额。

```
SELECT   车牌号码,年末千米数 - 年初千米数
FROM     出租车补贴数据;
```

(4) 指定别名改变查询结果的列标题。

查询“出租车补贴数据”中车牌号码和全年行驶里程,并把车牌号码显示为“License Plate Number”。

```
SELECT  车牌号码 AS License Plate Number, 全年行驶里程
FROM     出租车补贴数据;
```

2) 选择表中的若干元行

查询满足条件的元组:WHERE 子句。WHERE 子句的条件表达式中可使用的运算符有以下几种。

(1) 算术比较运算符:

```
= 、>、<、>= 、<= 、<>、!>、!<
```

① 查询“出租车补贴数据”中“单位名称”为“A 公司”的“车牌号码”。

```
SELECT  车牌号码
FROM  出租车补贴数据
WHERE  单位名称 = "A 公司";
```

② 查询“出租车补贴数据”中“全年行驶里程”在 3000 以下的“车牌号码”及“营运证号”。

```
SELECT 车牌号码,营运证号
FROM  出租车补贴数据
WHERE  全年行驶里程< 3000;
```

(2) 确定范围:

```
BETWEEN … AND … 和 NOT          BETWEEN … AND …
```

查询“出租车补贴数据”中“全年行驶里程”为 1000～3000(包括 1000 和 3000)的“车牌号码”“营运证号”及“全年行驶里程”。

```
SELECT 车牌号码,营运证号,全年行驶里程
FROM  出租车补贴数据
WHERE 全年行驶里程 BETWEEN 1000 AND 3000;
```

查询“出租车补贴数据”中“全年行驶里程”不为 1000～3000(包括 1000 和 3000)的“车牌号码”“营运证号”“全年行驶里程”。

```
SELECT 车牌号码,营运证号,全年行驶里程
FROM 出租车补贴数据
WHERE 全年行驶里程 NOT BETWEEN 1000 AND 3000;
```

(3) 确定集合(集合成员资格确认)运算符：

```
IN 和 NOT IN
```

① 查询“出租车补贴数据”中“单位名称”为“A 公司”“B 公司”“C 公司”的“车牌号码”“营运证号”“单位名称”。

```
SELECT 车牌号码,营运证号,单位名称
FROM 出租车补贴数据
WHERE 单位名称 IN("A 公司","B 公司","C 公司");
```

② 查询“出租车补贴数据”中“单位名称”不是“A 公司”“B 公司”“C 公司”的“车牌号码”“营运证号”“单位名称”。

```
SELECT 车牌号码,营运证号,单位名称
FROM 出租车补贴数据
WHERE 单位名称 NOT IN("A 公司","B 公司","C 公司");
```

(4) 字符匹配：

LIKE 表示字符串的匹配,其一般语法格式如下：

```
[NOT]LIKE "<匹配串>"
```

其含义是查找指定的属性列值与<匹配串>相匹配的元组。<匹配串>可以是一个完整的字符串,也可以含有通配符%和?。

其中,%代表任意长度(长度可以为 0)的字符串,例如,a%b 表示以 a 开头,以 b 结尾的任意长度字符串,例如,acb、addgb、ab。

?代表任一单个字符,例如,a?b 表示以 a 开头,以 b 结尾,长度为 3 的任意字符串,如 acb、afb。

① 查询“出租车补贴数据”中“车牌号码”为“江 K5T88”的所有信息。

```
SELECT   *
FROM 出租车补贴数据
WHERE 车牌号码 LIKE"江 K5T88";
```

等价于：

```
SELECT    *
FROM 出租车补贴数据
WHERE 车牌号码 = "江 K5T88";
```

如果 LIKE 后面的匹配串中不含通配符,则可以用“=”运算符取代 LIKE 谓词,用!=或<>运算符取代 NOT LIKE 谓词。

② 查询“出租车补贴数据”中“单位名称”里含有“A”的“车牌号码”及“营运证号”。

```
SELECT 车牌号码,营运证号
FROM 出租车补贴数据
WHERE 单位名称 LIKE "A%";
```

③ 查询“出租车补贴数据”中“单位名称”里含有“B”且全名为三个字符的“车牌号码”及“单位名称”。

```
SELECT 车牌号码,单位名称
FROM 出租车补贴数据
WHERE 单位名称 LIKE "B??";
```

④ 查询“出租车补贴数据”中“单位名称”里不含有“B”的“车牌号码”及“单位名称”。

```
SELECT 车牌号码,单位名称
FROM 出租车补贴数据
WHERE 单位名称 NOT LIKE "B%";
```

(5) 空值。

```
IS NULL
```

(6) 多重条件(逻辑运算符)。

```
AND,OR,NOT(可与其他类别运算符联合使用)
```

查询“出租车补贴数据”中“单位名称”为“A 公司”,“全年行驶里程”在 45000 以下的“车牌号码”及“营运证号”。

```
SELECT 车牌号码,营运证号
FROM    出租车补贴数据
WHERE 单位名称 = "A 公司" and 全年行驶里程< 45000;
```

3) 对查询结果排序

使用 ORDER BY 子句对查询结果按照一个或多个属性列的升序(ASC)或降序(DESC)排列,默认值为升序。

查询“出租车补贴数据”中“单位名称”为“A 公司”的“车牌号码”“ 营运证号”“全年行驶里程”,查询结果按“全年行驶里程”降序排列。

```
SELECT 车牌号码,营运证号,全年行驶里程
FROM 出租车补贴数据
WHERE 单位名称 = "A 公司"
ORDER BY 全年行驶里程   DESC;
```

4）对查询结果分组

GROUP BY 子句将查询结果表按某一列或多列值分组，值相等的为一组。

（1）查询“出租车补贴数据”中“车牌颜色”及相应的车辆数量。

```
SELECT 车牌颜色,COUNT(车牌颜色)
FROM 出租车补贴数据
GROUP BY 车牌颜色;
```

（2）查询“出租车补贴数据”中每种“车牌颜色”的“全年行驶里程”的总和。

```
SELECT 车牌颜色,SUM(全年行驶里程)
FROM 出租车补贴数据
Group BY 车牌颜色;
```

3.4　与信息系统审计相关的其他技术工具

1. 数据分析工具

数据分析是指用适当的统计分析方法对收集来的大量数据进行分析，将它们加以汇总和理解并消化，以求最大化地开发数据的功能，发挥数据的作用。数据分析是为了提取有用信息和形成结论而对数据加以详细研究和概括总结的过程。在审计工作中，除了 3.3 节介绍的 SQL 外，Excel、Python、R、Smartbi、Tableau、SPSS、SAS 等工具也被广泛使用。

2. 日志安全审计工具

日志安全审计目的是收集系统日志，通过从各种网络设备、服务器、用户计算机、数据库、应用系统和网络安全设备中收集日志，进行统一管理和分析。日志审计系统功能包括信息采集、信息分析、信息存储、信息展示等功能。当前信息安全形势日益严峻，信息安全防护工作面临前所未有的困难和挑战。日志审计能够帮助用户更好地监控和保障信息系统运行，及时识别针对信息系统的入侵攻击、内部违规等信息，同时日志审计能够为安全事件的事后分析、调查取证提供必要的信息。

目前，一些日志数据审计工具已经被开发出来，如 EventLog Analyzer。

3. 源代码安全审计工具

源代码安全审计是依据公共漏洞字典表、开放式 Web 应用程序安全项目以及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对各种程序语言编写的源代码进行安全审计。可提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、提出修改建议等一系列服务。

4. 网络安全审计工具

网络安全审计是指按照一定的安全策略，利用记录、系统活动和用户活动等信息，检查和检验操作事件的环境及活动，从而发现系统漏洞、入侵行为或改善系统性能的过程。也是检查评估系统安全风险并采取相应措施的一个过程。网络安全审计从审计级别上可分为三种类型：系统级审计、应用级审计和用户级审计。

小　结

(1) 信息系统审计方法与工具是审计人员为了完成信息系统审计任务所采取的各种手段。在信息系统审计工作中,要完成每一项审计工作,都应选择合适的审计方法与工具。

(2) 信息系统初步审查的方法主要包括访谈法、问卷调查法、检查法、观察法和风险评估法。通过这些方法的应用,信息系统审计人员应了解到被审信息系统的基本情况,明确审计重点和方向,为进一步实施审计打下基础。

(3) 经过多年的信息系统审计实践,国内外出现了许多计算辅助审计技术。在众多的计算机辅助审计技术中,应用最广泛的是数据测试和分析方法,按照是否处理实际业务数据来分,可以分为处理虚拟数据的程序测试方法和处理实际业务数据的程序测试方法两类。

(4) 处理虚拟数据的程序测试方法,特点是通过处理事先设计的测试数据来确定应用程序的可靠性。通过设计少量测试数据,对局部或大部分应用程序进行测试,也可根据需要对某特定控制措施进行测试。测试过程:①设计测试数据;②手工处理设计好的数据;③用被测试程序处理已设计好的数据;④比较上述两种方式处理的结果,并推断应用控制的可靠性。具体方法包括检测数据法与整体检测法。

(5) 处理实际数据的程序测试方法,特点是使用用户单位的计算机程序处理实际数据以确定应用控制可靠性。审计人员可以利用已形成的实际数据,无须再设计测试数据,而且用程序处理的结果能表明程序控制的强弱。具体方法包括受控处理法,受控再处理法,平行模拟法,嵌入审计程序法,程序追踪法(标记追踪法)。

(6) SQL 是一种数据库查询和程序设计语言,用于存取数据以及查询、更新和管理关系数据库系统。目前,绝大多数流行的关系型数据库管理系统,如 Oracle、Sybase、Microsoft SQL Server、Microsoft Access 都支持 SQL 作为查询语言。在开展信息系统审计的过程中会用到 SQL。

(7) 在信息系统审计工作中,除了 SQL 外,Excel、Python、R、Smartbi、Tableau、SPSS、SAS 等工具也被广泛使用。另外,本章最后还对一些与信息系统审计相关的其他特殊专业工具(日志安全审计工具、源代码安全审计工具、网络安全审计工具)等进行了介绍。

复习思考题

一、单选题

1. 对新的应收账模块实施实质性审计测试时,信息系统审计人员的日程安排非常紧,而且对计算机技术知之不多。那么,下面哪一项审计技术是最佳选择?(　　)

A. 测试数据　　B. 平行模拟(parallel simulation)

C. 整体测试法(ITF)　　D. 嵌入式审计模块(EAM)

2. 下列哪一项是执行平行测试的最重要目的?(　　)

A. 决定系统是否有成本效益　　B. 使全面的单元和系统测试成为可能

C. 突出文件程序接口的错误　　D. 确保新系统满足客户需求

3. 一个程序员恶意地修改了生产程序代码以改变数据，随后又恢复了源代码。下列哪一项是发现这个恶意行为的最有效的方法？（　　）

A. 比较源代码　　B. 检查系统日志文件

C. 比较目标代码　　D. 比较可执行代码和源代码的完整性

4. 在审查客户主文件的时候，信息系统审计人员发现很多客户的名字相同，为了进一步确定重复程度，IS 设计师应该（　　）。

A. 测试数据以确认输入数据

B. 测试数据以确定系统排序能力

C. 用通用审计软件确定地址字段的重复情况

D. 用通用审计软件确定账户字段的重复情况

5. 检查 IT 战略规划过程时，信息系统审计人员应该确保这个规划（　　）。

A. 符合技术水平现状　　B. 匹配所需的操作控制

C. 明晰 IT 的任务与远景目标　　D. 详细说明项目管理实务

6. 下面哪一项用于描述 ITF(整体测试法)最合适？（　　）

A. 这种方法使信息系统审计人员能够测试计算机应用程序以核实正确处理

B. 利用硬件或软件测试和审查计算机系统的功能

C. 这种方法能够使用特殊的程序选项打印出通过计算机系统执行的特定交易的流程

D. IS 系统审计人员用于测试的一种程序，可以用于处理标签和扩展交易和主文件记录。

7. 信息系统审计人员要判断是否严格控制被授权者对于程序文档的访问，最有可能的做法是（　　）。

A. 评估在存储场所的文件保存计划

B. 就当前正在进行的流程采访程序员

C. 对比实际使用的记录和操作表

D. 审查数据文件访问记录测试管理库的功能

8. 证明税收计算系统精确性的最好的方法是（　　）。

A. 对于计算程序源代码详细目测审核和分析

B. 使用通用审计软件对每个月计算的总数进行重复的逻辑计算

C. 为处理流程准备模拟交易，并和预先确定的结果进行比较

D. 自动分析流程图和计算程序的源代码

9. 以下哪一个是使用测试数据的最大挑战？（　　）

A. 确定测试的程序的版本和产品程序的版本一致

B. 制造测试数据包括所有可能的有效和无效的条件

C. 对于测试的应用系统，尽量减少附加交易的影响

D. 在审计人员监督下处理测试数据

10. 以下哪一个是使用 ITF 综合测试法的优势？（　　）

A. 使用真实的或虚拟的主文件，信息系统审计人员不需要审查交易的来源

B. 定期检验过程并不需要单独分离测试过程

C. 证实应用程序并可测试正在进行的操作

D. 它无须准备测试数据

二、填空题

1. 审计访谈按照访谈过程的控制程度划分为_____和_____。

2. 在风险评估时可以选择多种风险分析技术，可采用_____，也可以采用_____。风险分析的标准可以是简单的定性分类，也可以通过复杂的科学计算进行定量计算。

3. 根据审计风险理论，任何风险都是多因素集合作用的结果，审计风险也不例外，审计风险由_____、_____和_____三个要素构成。

4. 在众多的计算机辅助审计技术中，应用最广泛的是数据测试分析方法，按照是否处理实际业务数据来分，可以分为_____的程序测试方法和_____的程序测试方法两类。

5. _____是指审计人员通过被审程序对实际会计业务的处理进行监控，查明被审程序的处理和控制功能是否恰当、有效的方法。

三、简答题

1. 信息系统初步审查的方法有哪些？简述每种方法的内容及其优缺点。

2. 简述信息系统审计风险评估的操作步骤。

3. 简述计算机辅助审计技术的概念与特点。

4. 简述检测数据法的原理。

5. 整体检测法有哪些优点与缺点？

6. 简述平行模拟法的概念和优缺点。

7. 开展信息系统审计为什么需要了解 SQL 的基本知识？