



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

# 会计信息系统的控制和审计

饶艳超 上海财经大学会计学院

[raoyanchao@qq.com](mailto:raoyanchao@qq.com)





- 学习目标

- 了解信息系统审计的相关概念
- 熟悉信息系统审计步骤和审计内容
- 了解并熟悉COSO内部控制框架和企业风险管理框架
- 熟悉并学会应用常用的信息系统审计工具和技术
- 熟悉会计信息系统的一般控制和应用控制内容及要求
- 学会进行会计信息系统的一般控制和审计
- 学会进行会计信息系统的应用控制和审计
- 熟悉并尝试应用信息系统审计准则的主要框架和内容



- 内部控制的发展
  - 萌芽期——内部牵制
  - 发展期——内部会计控制与内部管理控制
  - 成熟期——内部控制结构和内部控制整体架构



- 内部控制的定义

- 内部控制结构

- 1988年4月美国注册会计师协会发布的《审计准则公告第55号(SAS NO.55)——“财务报表审计对内部控制结构的考虑”，规定从1990年1月起以该文告取代1972年发布的《审计准则公告第1号》。该文告首次以内部控制结构(Internal Control Structure)一词取代原有的“内部控制”一词。
    - “企业内部控制结构包括为合理保证企业特定目标的实现而建立的各种政策和程序”



- 内部控制的定义

- 内部控制结构

- 内部控制结构的内容，三要素结构具体包括：

- 控制环境：指对建立、加强或削弱特定政策和程序效率发生影响的各种因素。
      - 会计系统：规定各项经济业务的鉴定、分析、归类、登记和编报的方法，明确各项资产和负债的经营管理责任。
      - 控制程序：管理当局所制订的用以保证达到一定目的的方针和程序。



- 内部控制的定义

- 内部控制整体框架

- **1992年COSO 委员会提出《内部控制——整体架构(Internal Control—Integrated Framework)》**，也称**COSO报告**。
    - **1994年提出的修改篇**，扩大了内部控制涵盖范围，增加了与保障资产安全有关的控制。
    - **AICPA全面接受COSO报告的内容**，于**1995年**据以发布了《审计准则公告第**78号**》(**SAS NO.78**)，并自**1997年1月**起取代了《审计准则公告第**55号**》。
    - **COSO报告指出:内部控制是一个过程**，受企业董事会、管理当局和其他员工影响，旨在保证财务报告的可靠性、经营的效果和效率以及现行法规的遵循。
      - 内部控制整体架构主要由控制环境、风险评估、控制活动、信息与沟通、监督五项要素构成。



- **COSO内部控制框架**

- 控制环境的因素具体包括:

- 1.诚信的原则和道德价值观。
    - 2.评定员工的能力。
    - 3.董事会和审计委员会。
    - 4.管理哲学和经营风格。
    - 5.组织结构。
    - 6.责任的分配与授权。
    - 7.人力资源政策及实务。





- **COSO内部控制框架**

- 评估风险的先决条件，是制定目标。风险评估就是分析和辨认实现所定目标可能发生的风险。

- 1.目标。

- 2.风险。

- 3.环境变化后的管理。





- **COSO内部控制框架**
  - 控制活动，是确保管理层的指令得以执行的策略及程序，如核准、授权、验证、调节、复核营业绩效、保障资产安全及职务分工等。
  - 控制活动在企业内的各个阶层和职能之间都会出现，这主要包括：
    - 1.高层经理人员对企业绩效进行分析。
    - 2.直接部门管理。
    - 3.对信息处理的控制。
    - 4.实体控制。
    - 5.绩效指标的比较。
    - 6.分工。



- COSO内部控制框架

- 信息与沟通

- 企业所有员工必须从最高管理阶层清楚地获取承担控制责任的信息，而且必须有向上级部门沟通重要信息的方法，并对外界顾客、供应商、政府主管机关和股东等做有效的沟通。
  - 1.信息系统。
    - 信息系统处理企业内部信息和外部信息。
  - 2.沟通。
    - 企业的信息系统提供有效信息给适当的人员，通过沟通，使员工能够知悉其营业、财务报告及遵循法律的责任。
    - 企业沟通包括内部沟通和外部沟通。



- COSO内部控制框架

- 监督

- 内部控制系统需被监督。
    - 监督是由适当的人员，在适当及时的基础下，评估控制的设计和运作情况的过程。
    - 1.持续的监督活动。持续的监督活动在营运过程中发生，它包括例行的管理和监督活动，以及其他员工为履行其职务所采取的行动。
    - 2.个别评估。
    - 3.报告缺陷。



- 企业风险管理框架

- 强调内部控制框架的建立应与企业的风险管理相结合
- 新的企业风险管理框架就是在1992年的研究成果——《内部控制框架》报告的基础上，结合《萨班斯—奥克斯法案》(Sarbanes—Oxley Act)在报告方面的要求，进行扩展研究得到的。
- 普华永道的项目参与者认为，新报告中有60%的内容得益于COSO1992年报告所做的工作。
- 相对于内部控制框架而言，新的COSO报告新增加了一个观念、一个目标、两个概念和三个要素，即“风险组合观”、“战略目标”、“风险偏好”和“风险容忍度”的概念以及“目标制定”、“事项识别”和“风险反应”要素。



- 企业风险管理框架

- 1. 企业风险管理的定义

- 一个过程，其本身并不是一个结果，而是实现结果的一种方式。
    - 一个由人参与的过程，涉及一个企业各个层次员工。
    - 该过程可用于企业的战略制定。

- 2. 风险管理目标和要素

- 企业的风险管理框架包括四类目标和八要素。
    - 四类目标分别是战略目标、经营目标、报告目标和合法性目标。
    - 八要素是内部环境、目标制定、事项识别、风险评估、风险反应、控制活动、信息和沟通、监控，是企业实现各类目标的保证，它们相互之间存在直接的关系。



- 企业风险管理框架

- 企业风险管理框架新增了三个风险管理要素——“目标制定”、“事项识别”和“风险反应”。
- 1.目标制定——在风险管理框架中，要针对不同的目标分析其相应的风险，目标的制定自然就成为风险管理流程的首要步骤
  - 企业风险管理和内部控制框架都承认风险来自于企业内、外部各种因素，而且可能在企业的各个层面上出现，并且应根据对实现企业目标的潜在影响来确认风险。



- 企业风险管理框架

- **2.事项识别——企业风险管理框架深入探讨了潜在事项的概念，认为潜在事项是指来自于企业内部和外部资源的，可能影响企业战略的执行和目标实现的一件或者一系列偶发事项。**
  - 存在潜在的积极影响的事项代表机遇，而存在潜在负面影响的事项则称为风险。
  - 企业风险管理框架采用一系列技术来识别有关事项并考虑有关事项的起因，对企业过去和未来的潜在事项以及事项的发生趋势进行计量。





- 企业风险管理框架

- **3.风险反应(Risk Response)。**企业风险管理框架提出对风险的四种反应方案：规避、减少、共担和接受风险。

- 作为风险管理的一部分，管理者应比较不同方案的潜在影响，并且应在企业风险容忍度范围内的假设下，考虑风险反应方案的选择。
- 在个别和分组考虑风险的各反应方案后，企业管理者应从总体的角度考虑企业选择的所有风险反应方案组合后对企业的总体影响。



- 企业风险管理框架

- 4.风险评估。

- 内部控制框架和风险管理框架都强调对风险的评估，但风险管理框架建议更加透彻地看待风险管理，即从固有风险和残存风险的角度来看待风险，对风险影响的分析则采用简单算术平均数、最差的情形下的估计值或者事项的分布等技术来分析。
    - 风险评估的时间基准应与企业的战略和目标相一致，如果可能，也应与可观测到的数据相一致。
    - 企业风险管理框架还要求注意相互关联的风险，确定单一的事项如何为企业带来多重的风险。



- 企业风险管理框架

- 5.信息和沟通。

- 企业风险管理框架扩大了企业信息和沟通的构成内容，认为企业的信息应包括来自过去、现在和未来潜在事项的数据。
    - 企业的信息系统的基本职能应以时间序列的形式收集、捕捉数据，其收集数据的详细程度则视企业风险识别、评估和反应的需要而定，并保证将风险维持在风险偏好的范围内。



- 3. 各管理层在企业风险管理中的地位和职责

- (1)董事会：董事会对企业的风险管理负有监督职责
- (2)管理者：首席执行官对企业的风险管理最终负责。
- (3)风险管理员：与企业内其他管理者一起，在各自的职责范围内建立并维护有效的风险管理框架。
- (4)内部审计人员：在企业风险管理的监控中占有重要的地位，这一职责是其日常职责的一部分。
- (5)其他员工：企业风险管理是企业内每一个员工的责任，因此，风险管理应是企业内每一个员工的工作手册的一部分内容。



## 业务过程控制

- 业务过程是会计信息系统的处理对象，也是会计信息系统输入数据的来源和输出信息的终点
- 要对会计信息系统进行有效的控制，必须对业务过程进行控制，而且会计信息系统控制因为服务于业务过程，因此对业务过程控制的控制必然要考虑会计信息系统控制。
- 企业控制系统，一般适宜按照业务循环划分为子控制系统，当然实际工作中的业务循环划分及其取舍，主要取决于企业业务特征与需求。



- 1、一般控制
  - (1) 组织控制
  - (2) 操作控制
  - (3) 硬件控制
  - (4) 软件控制
  - (4) 数据安全控制
  - (5) 应用系统开发和维护控制



- 组织控制指采取职能分离、合理分工等手段保证电算化信息系统运营正常。
- 一、电算化部门 and 用户部门职能的分离
  - （一）用户部门的职能
  - （二）电算化部门的职能
  - （三）用户部门和电算化部门之间的关系
  - （四）对错误的处理方法





# 组织控制



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、电算化部门内部的职能分离
  - （一）电算化信息系统开发小组
  - （二）电算化信息系统使用小组



# 组织控制



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 三、加强对员工的管理
  - （一）强化安全意识
  - （二）识别敏感岗位
  - （三）加强对敏感岗位的控制
  - 需要格外关注和注意观察的情形
- 四、财政部关于电算化会计工作中组织控制方面的规定



- 操作控制指通过操作手册和操作系统等的严格规定和遵从，从而保证电算化信息系统操作上的正确性。
- 一、操作控制的基本内容
  - （一）严格的上机操作手册
  - （二）严格的软件操作规程
  - （三）硬件和软件的使用记录制度
  - （四）系统的运行指标的考核
  - （五）定期的维护和保养
  - （六）系统错误记录和分析报告
  - （七）保证机房设施安全和电子计算机正常运转的措施
  - （八）会计数据和会计核算软件安全保密的措施



- 二、财政部关于电算化会计工作中操作控制方面的规定
  - （一）建立会计电算化操作管理制度
  - （二）建立计算机硬件、软件和数据管理制度



- 一、硬件的安全
- （一）硬件运行环境的控制
  - 1、机房环境
  - 2、火灾
  - 3、水灾
  - 4、灰尘
  - 5、恶劣天气
  - 6、电磁波
  - 7、静电



- (二) 硬件防护
  - 1、计算机对供电电源的要求
    - (1) 直接供电
    - (2) 经过隔离变压器供电
    - (3) 交流稳压器供电
    - (4) 不间断电源 (UPS) 供电
  - 2、双重系统



- (三) 硬件接触控制
  - 1、机房地址不要选择在人流热闹的地方。
  - 2、对机房加锁。
  - 3、对进出机房的人采用身份识别技术。
  - 4、采用闭路电视进行多角度的监控。
  - 5、计算机设备上可以加上标签，这样当有人试图将其带出时，会发出警报。





- 二、软件的安全
- （一）软件的接触控制
  - 1、采用口令控制方式
    - （1）口令应该定期更改。
    - （2）口令的位数不应该过短。
    - （3）口令的设置不要和使用者的个人情况有太多的联系。
    - （4）口令不要传播给别人。
    - （5）系统要对口令输错的情况进行监控和分析，防止有人蓄意试探口令。
  - 2、采用权限控制方式



- 二、软件的安全
- (二) 防止计算机病毒的侵害
  - 1、加强机房管理，避免使用来路不明的软盘和非法拷贝的软件，也不要接收异常的电子邮件，在下载时也要小心；
  - 2、购置反病毒软件，经常对硬盘和软盘进行病毒检测；
  - 3、对重要资料进行经常的备份；
  - 4、确定自己的危险程度，制定一旦病毒入侵需要采取的方案，制定相应的恢复措施。
  - 公安部于2000年发布的《计算机病毒防治管理办法》



- 三、数据的安全
- （一）数据的接触控制
  - 1、口令控制方式
  - 2、加强对存储介质的管理
  - 3、磁介质上数据的加密保护
    - 硬加密技术



- 三、数据的安全
- （二）数据的加密
  - 1、数据的加密和解密
    - （1）密钥的管理
    - （2）加密/解密算法的设计
  - 2、数据的完整性



- 三、数据的安全
- （三）数据的备份制度
  - 1、临时的方法：偶尔将个人文件拷贝到软盘上。
  - 2、谨慎的方法：定期进行备份拷贝。
  - 3、专业的方法：祖父/父亲/儿子方案。
- （四）防止计算机病毒的侵害



- 四、人员的安全
  - 工作在电算化信息系统环境下的人员可能会遭到一些安全问题。
  - 重复性紧张损伤
  - 应该考虑人类工程学。



# 财政部的相关规定



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- （一）《会计电算化工作规范》中的相关规定
- （二）《会计核算软件基本功能规范》中的相关规定





# 会计信息系统一般控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 一、电算化信息系统一般控制的审计重点
  - （一）物理安全方面
  - （二）逻辑安全安全
  - （三）备份
  - （四）灾难恢复
- 二、对电算化信息系统一般控制的调查



# 会计信息系统的应用控制和审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

## 应用控制概述

- 每一个具体的应用程序所要解决的问题是不同的，所涉及到的数据和处理方法等均各具特点。针对这些具体的应用程序所进行的有针对性的控制，就是应用控制。
- 应用控制和一般控制是相互支持的。一般控制着重于对整体环境的控制，而应用控制着重于对其中具体环节的控制。
- 应用控制内容
  - (1) 输入控制
  - (2) 计算机处理与数据文件控制
  - (3) 输出控制
- 应用控制的审计



# 应用控制目的



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 应用控制的目的在于：
  - 1、保证所有经过审核批准的交易均经处理完毕，并且每一项交易只处理一次。
  - 2、保证交易资料的完整和正确。
  - 3、保证交易的处理正确无误，符合要求。
  - 4、保证处理的结果用于预定的用途，并能产生预期的效益。
  - 5、保证应用程序能正常运作，并持续维护其功能。



- 一、输入控制的重要性
  - 应用控制最为强调的控制环节就是输入环节的控制。
- 二、信息系统的输入
  - （一）计算机的处理类型
  - （二）计算机系统的输入阶段
- 三、会计信息系统的输入环节
  - 会计信息系统的输入方式主要有采用键盘手工输入、软盘转入和网络传输等几种。



- 输入控制
  - （一）账务处理模块的输入环节
  - （二）其他业务核算模块的输入环节



- 四、会计信息系统的输入控制方法
- 输入控制的目的是保证输入工作的正确性、完整性和经过授权。
- 输入控制要针对输入数据中的重要字段进行。



- 四、会计信息系统的输入控制方法
  - （一）批控制总数的方法
  - （二）输入画面友好
  - （三）存在性校验
  - （四）校验位校验
  - （五）对应关系检查
  - （六）平衡关系校验
  - （七）界限、极值校验
  - （八）完整性校验
  - （九）连续性校验
  - （十）静态检查法
  - （十一）二次输入法



- 五、会计信息系统输入控制中要注意的问题
- 这些控制方法并不能够保证会计信息系统的输入环节完全正确。
- 这些方法的综合运用要比单独只采用某一种方法要好，更为全面。
- 另外，对于在输入控制中检查出来的错误信息的处理，必须非常慎重。





# 输入控制



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 五、会计信息系统输入控制中要注意的问题
- 六、财政部对于输入控制的具体规定



- 一、处理控制的目的
- 处理控制的目的是要：
  - 保证信息系统的处理按照各个模块所预先设定的程序进行，这些处理活动必须经过授权
  - 所有经过授权的处理都被系统进行过而没有遗漏，任何未经授权的处理都没有进行过
  - 在整个处理的过程中是正确的、及时的、有效的。



- 二、信息系统的处理
- 信息系统中对数据的加工处理方法包括分类、汇总、合并、排序等。
- 目前用于描述模块内部处理过程的主要方法。
  - （一）结构化英语（**Structured English**）
  - （二）决策表（**Decision Tree**）
  - （三）决策树（**Decision Table**）



- 三、会计信息系统的处理环节
- 会计信息系统中的**账务处理模块**的**处理工作**包括编制凭证、登记账簿、编制报表。
- 对于**工资核算模块**来说，主要的处理工作是计算各个员工的应发工资和实发工资，逐级汇总各个部门的工资发放情况，并进行工资的分配，同时产生相应的计提工资转账凭证。



- 三、会计信息系统的处理环节
- 对于**固定资产模块**来说，主要的处理工作是计提折旧。要根据固定资产上月末或本月初的余额、当前的折旧率与使用状态计算折旧，同时产生相应的计提折旧转账凭证。
- 对于**存货核算模块**，其工作流程主要就是存货的收、发、存工作，同时产生相应的转账凭证。等等。
- 总的来说，**各个业务核算模块的处理工作根据业务的不同各有不同的侧重点和流程及处理方法，但都要产生相应的转账凭证以便作为账务处理模块的输入。**



- 四、会计信息系统的处理控制方法
- 处理控制往往包含在计算机程序之中。
- 所能检查或者防止的错误类型包括：
  - 1、未将所有有待处理的数据加以处理，或将某些数据重复处理了多次。
  - 2、处理了其他的数据。
  - 3、对不合理的或不合逻辑的数据进行处理。
  - 4、在处理过程中遗漏或者损坏资料。



- 四、会计信息系统的处理控制方法
  - （一）控制总数的方法
  - （二）文件标签检查
  - （三）界限、极值校验
  - （四）平衡及勾稽关系校验



- 五、会计信息系统处理控制中要注意的问题
  - 由于硬件、软件、操作等方面的问题，依然会造成计算机自动处理的结果有误。处理控制不能放松。
  - 关键是掌握方法本身，而不需要去过于追究方法到底是用于输入控制还是处理控制。
  - 对于处理控制中发现的错误，必须分别情况进行处理：
    - （一）错误可以立即更正
    - （二）错误必须返回用户部门进行更正
    - （三）错误已经对主文件造成影响
- 六、财政部对于处理控制的具体规定





- 一、输出控制的目的
- 从系统的角度来看，输入和输出是相对的。
- 输出分为两种，一种是中间性的输出，一种是最终的面向用户的输出。
- 输出对用户来说是至关重要的。
- 输出控制的目的是要保证信息系统所处理的资料完整、正确，所处理的结果正确，并且保证只有经过授权的部门和人员才能获得这些输出资料。



- 二、信息系统的输出
- 信息系统常见的输出方式有两种：
  - 打印输出
  - 查询输出
- 输出的格式通常有三种
  - 简单形式输出
  - 棋盘式表格输出
  - 图形输出



- 三、会计信息系统的输出环节
- 会计信息系统中的账务处理模块应当提供对机内会计数据的查询功能。
- 账务处理模块还必须提供会计凭证、会计账簿、会计报表的打印输出功能。
- 工资核算模块应当可以输出有关工资的各类汇总表、工资单、工资分配表等。



- 三、会计信息系统的输出环节
- 固定资产核算模块可以根据用户自行设定的项目进行固定资产的分类、汇总、查询和统计，并打印输出有关固定资产的账册或表格等等。
- 在其他业务核算模块的输出中，还包括根据有关业务自动生成的机制凭证的输出。
- 另外，商品化会计软件必须充分考虑用户实际使用的各类打印机的情况，必须具有与各类打印机控制代码互相转换的功能，供用户使用。



- 四、会计信息系统的输出控制方法
- （一）输出信息内容和格式的控制
  - 输出信息必须符合用户的要求。
  - 在内容上，要做到有用、完整、正确、及时。
  - 为了对内容进行控制，要求电算部门在将输出信息传递给用户之前，先要进行控制总数等方法的校验。
  - 输出信息的格式也必须符合用户的要求。



- 四、会计信息系统的输出控制方法
- （二）输出信息传送过程的控制
- 必须对输出信息的传送进行控制。
  - 如果采用的是查询的输出方式
  - 如果采用的是打印的输出方式



- 五、会计信息系统输出控制中要注意的问题
  - 在会计信息的输出过程中必须同时注意两方面的控制，一个是内容和格式，一个是传送途径。只有这样，才能保证经过授权的用户得到了所需要的资料。
  - 如果输出控制中发现错误，同样需要对这些错误进行登记，分析错误的产生原因，并做出相应的补救措施。
- 六、财政部对于输出控制的具体规定



# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 一、电算化会计信息系统应用控制的审计重点
- 对电算化会计信息系统应用控制的审计，目的在于评价应用控制是否对该电算化信息系统的具体应用环节进行了保护和控制。主要要审查以下几个方面：
- （一）输入控制方面
- 实践证明输入环节是最容易出现错误的环节。为了保证电算化会计信息系统在起点的正确性，必须加强输入控制。





# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 一、电算化会计信息系统应用控制的审计重点
- （二）处理控制方面
- 计算机在将输入数据转化为输出结果的过程中，会受到各种因素的干扰，必须采取必要措施确保处理过程是正确无误的。



# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 一、电算化会计信息系统应用控制的审计重点
- （三）输出控制方面
- 对输出的控制分为两个方面，一是对输出的内容和格式的控制，二是对输出结果的管理控制。必须从这两个方面进行考察。



# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、对电算化会计信息系统应用控制的调查和测试
- （一）对应用控制制度的了解和描述
- 应用控制方法大多设计在相应的应用程序中。描述应用控制的方法既可以用程序流程图，也可以用问题式调查表，或者将两者结合起来使用。



# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、对电算化会计信息系统应用控制的调查和测试
- （二）对应用控制制度的初步评价
- 评价应用控制制度的标准是：内部控制是否健全、所有的控制目标是否已经达到、各项控制制度是否符合内部控制基本原则的要求。
- 要评价内部控制的合理性。合理性既需要考虑有效性，也需要考虑“成本、效益”原则。只有当系统的执行者具有相当好的素质和丰富的经验时，电算化会计信息系统才能很好地执行各项内部控制制度。



# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、对电算化会计信息系统应用控制的调查和测试
- （三）内部控制的测试
- 1、符合性测试
- 符合性测试着重要了解和评价会计信息系统所产生的会计数据的正确性。
- 具体方法是通过检查原始凭证、重做业务过程或者仔细观察应用系统运行状况来确定内部控制制度是否合理。



# 会计信息系统应用控制的审计



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、对电算化会计信息系统应用控制的调查和测试
- （三）内部控制的测试
- 2、实质性测试
- 对应用系统的应用控制采用一定的数据进行测试时，所用的数据可以是正确的数据，也可以是不正确的数据。
- 其目的在于测试应用系统的内部控制制度是否健全并是否能有效地执行。



# 会计信息系统测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 对程序文件的测试
- 对数据文件的测试



# 程序文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 一、电算化会计信息系统中的程序文件
- 在系统设计阶段得到的模块结构图
- 在系统实施阶段，用具体的程序文件来实现这些模块的功能。
- 电算化会计信息系统中，程序文件可以分为两大类。
  - 第一类是菜单程序
  - 第二类是具体业务程序





- 二、电算化会计信息系统中程序文件的测试
- （一）不运行程序文件的测试方法
- 1、查阅开发性文档
  - （1）模块结构图
  - （2）程序结构图
  - （3）IPO图
  - （4）源程序代码
  - （5）系统测试和调试记录



- 二、电算化会计信息系统中程序文件的测试
  - （一）不运行程序文件的测试方法
    - 2、查阅使用性文档
      - （1）操作说明书等
      - （2）操作日志
    - 3、查阅维护性文档
      - 软件维护分为四种情况：改正性维护、适应性维护、完善性维护和预防性维护。
  - 不运行程序文件的测试方法的优缺点



- 二、电算化会计信息系统中程序文件的测试
- （二）运行实际数据的测试方法
- 1、实际数据的测试方法
- 采用运行实际数据的测试方法是指在测试程序文件的时候采用的测试数据是被测试企业实际发生的数据。
- 这种方法的最大优点首先是真实，另外由于测试用的数据是实际数据，所以较易获得。



- 二、电算化会计信息系统中程序文件的测试
- （二）运行实际数据的测试方法
- 1、实际数据的测试方法
- 这种方法也存在的一些问题：
  - （1）实际的数据虽然是上个会计期间或者这个会计期间的真实数据，但这两个会计期间的数据并不一定完全反映出所有会计期间的数据的特征。
  - （2）审计人员的观察或者实际操作必然会影响到或干扰被审计企业的工作，由此得到的观察或者操作结果是否足以代表被审计企业的一贯情况呢？



- 二、电算化会计信息系统中程序文件的测试
- （二）运行实际数据的测试方法
- 1、实际数据的测试方法
- 这种方法也存在的一些问题：
  - （3）审计人员并不能够确认被审计企业提交给审计人员的程序文件就是真实的在用的程序文件；
  - （4）审计人员必须对程序处理过程非常熟悉，才能够全面地实施和监控测试过程；
  - （5）这种测试方法所需要记录的工作底稿的内容很多，较琐碎。

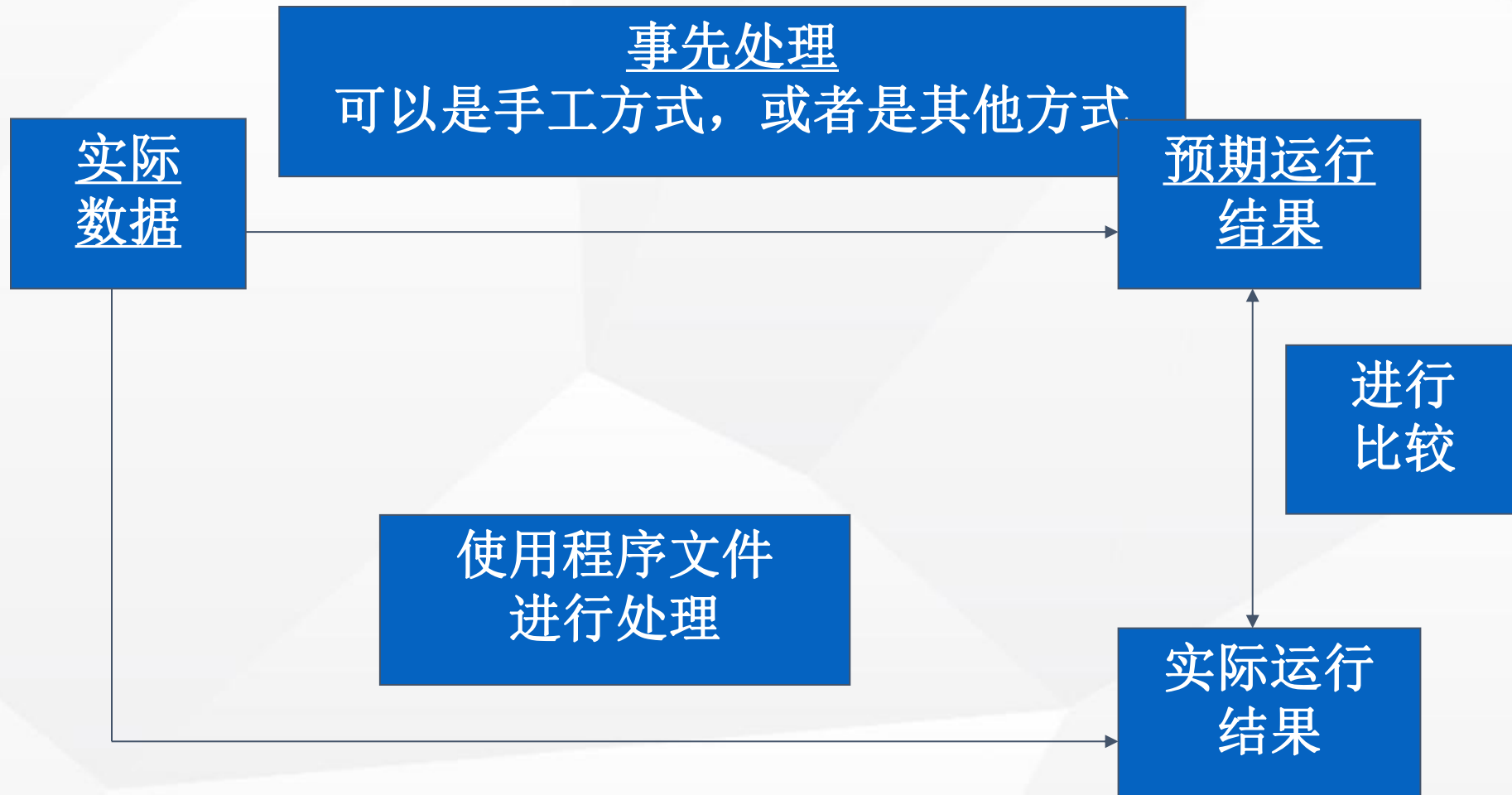


- 二、电算化会计信息系统中程序文件的测试
- （二）运行实际数据的测试方法
- 2、具体的测试技术
- （1）受控处理法
  - 受控处理法是指审计人员在实际的会计数据处理的过程中进行控制。
  - 优点：受控处理法比较直观明了，易于理解。
  - 缺点：可能对被审计企业正常工作造成干扰和影响。



# 程序文件测试

- (1) 受控处理法





- 2、具体的测试技术
- (2) 受控再处理法
  - 受控再处理法和上述受控处理法基本相同。
  - 主要区别在于受控处理法中是对数据的第一次输入、处理和输出的过程进行监控，而受控再处理法则是对已经经过输入、处理和输出的数据进行再一次的输入、处理和输出，对第二次过程进行监控。
  - 同样，这种方法也是要确认输入、处理和输出的控制的有效性。
  - 优缺点



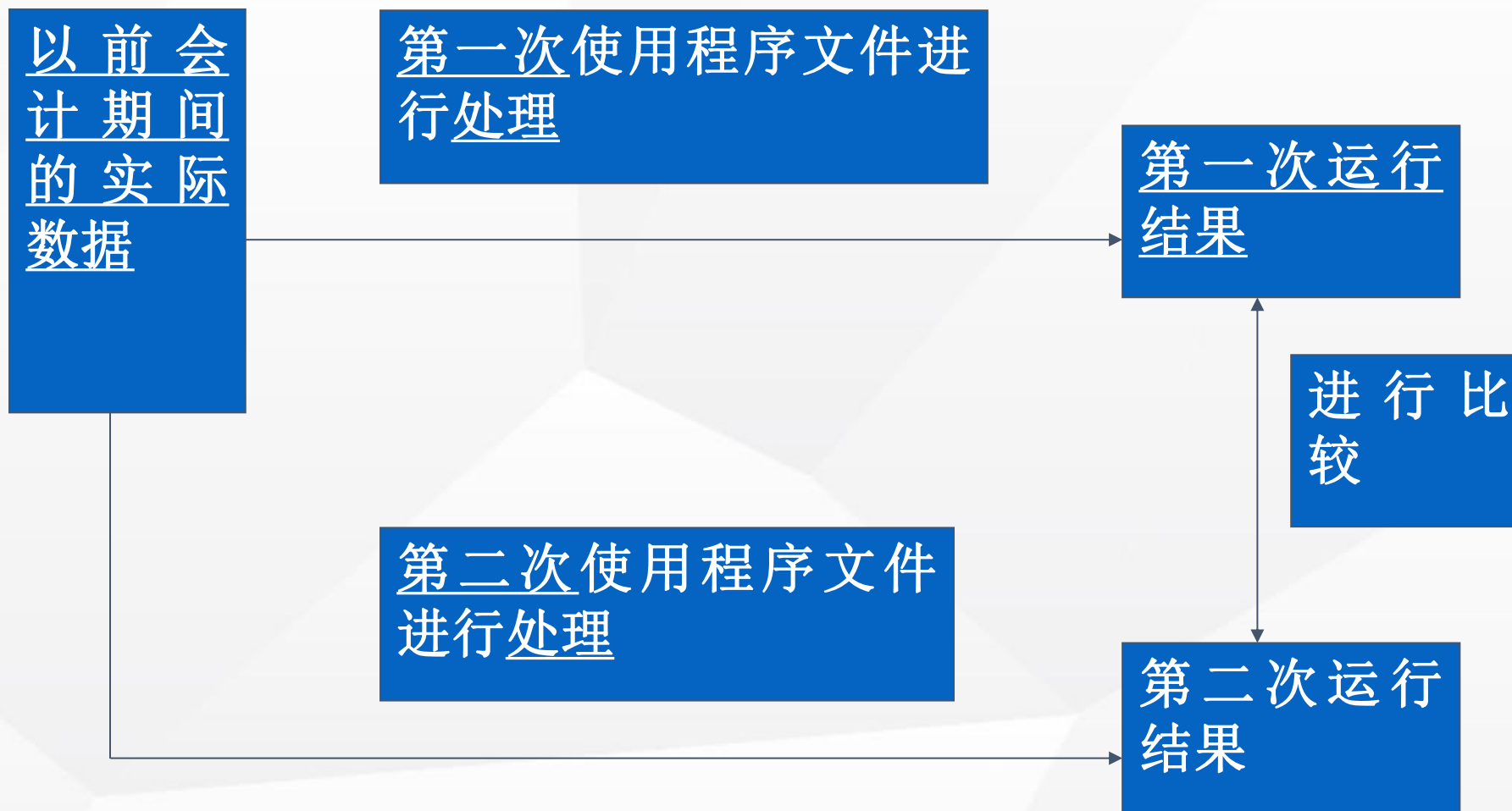


# 程序文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- (2) 受控再处理法





- 2、具体的测试技术
- (3) 平行模拟法
  - 平行模拟法是指审计人员事先获得一个和被审计程序文件同样功能的模拟程序，然后将有待处理的会计数据在这个模拟程序上和被审计的程序文件上同时进行处理，比较这两个处理的过程和结果，以此判断被审计程序的控制的有效性。
  - 优缺点



# 程序文件测试

- (3) 平行模拟法





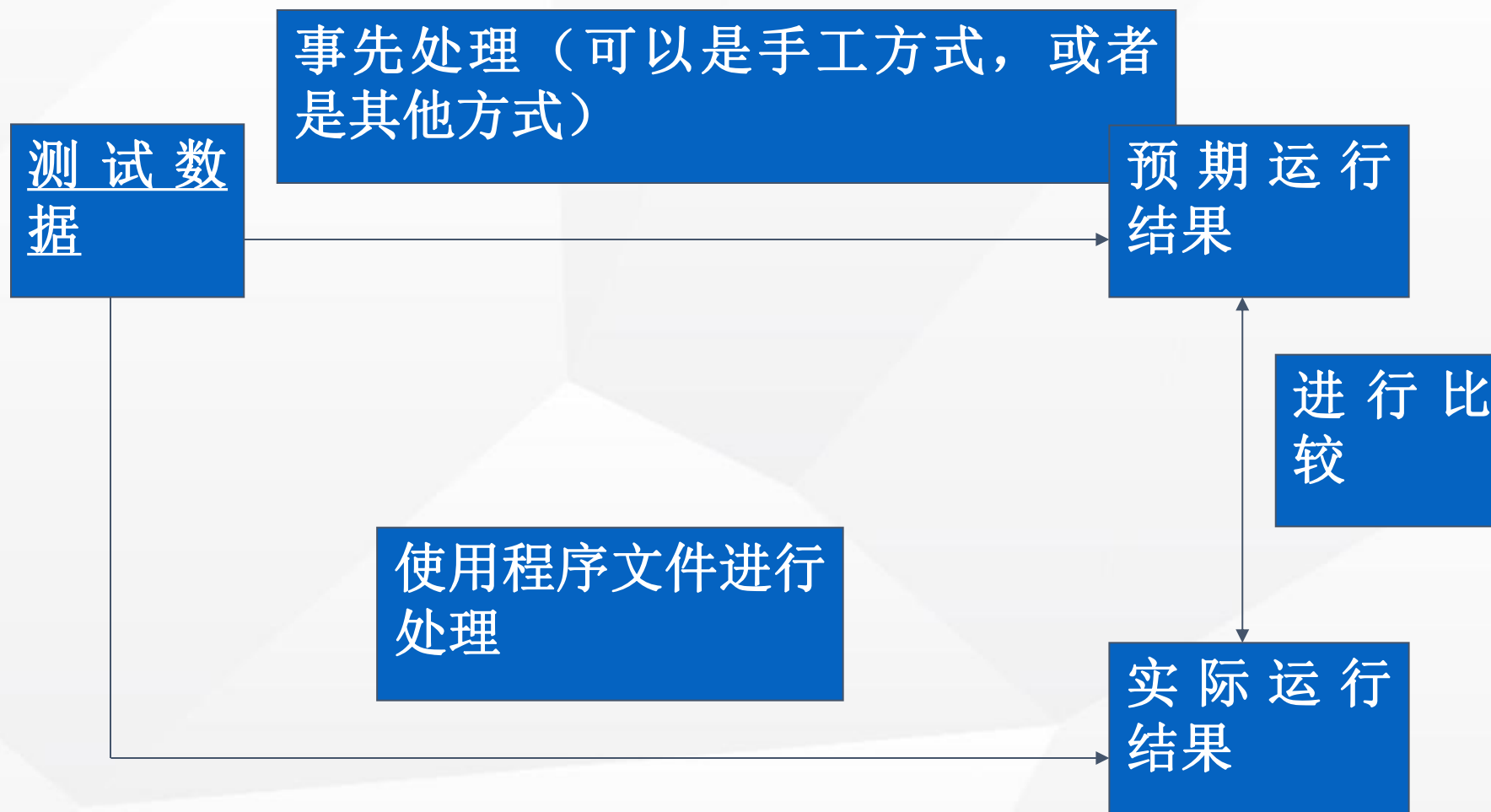
- 二、电算化会计信息系统中程序文件的测试
- （三）运行模拟数据的测试
- 1、模拟数据的测试方法
  - 通过编制一些模拟数据来测试某项控制措施是否存在。
  - 优缺点
- 2、具体的测试技术
  - （1）测试数据法
    - 审计人员模拟出一批测试数据，并用手工方法得到测试数据的预期处理结果。然后审计人员将这些测试数据交由被审计企业的程序文件进行处理。程序文件处理后得到的结果和事先预期的结果进行比较，并对可能存在的差异进行分析。



# 程序文件测试



- (1) 测试数据法





• (1) 测试数据法记账凭证输入程序中测试数据法举例

测试数据编号	要测试的控制措施	测试数据	预期结果
1	记账凭证编号的连续性	输入一张记账凭证，使其凭证编号和已经存在的某张凭证编号相同，其他项目正常	检测出来，不予处理，并给出错误信息
2	记账凭证上会计科目的存在性	输入一张记账凭证，使其会计科目在企业会计科目代码库中查找不到，其他项目正常	检测出来，不予处理，并给出错误信息
3	记账凭证上会计科目的校验位	输入一张记账凭证，使其会计科目出现窜位错误，其他项目正常	检测出来，不予处理，并给出错误信息



• (1) 测试数据法记账凭证输入程序中测试数据法举例

测试数据编号	要测试的控制措施	测试数据	预期结果
4	记账凭证上会计科目对应关系	输入一张记账凭证，使其借贷方会计科目出现非法对应关系，其他项目正常	检测出来，不予处理，并给出错误信息
5	记账凭证上凭证种类和会计科目之间的关系	输入一张记账凭证，使其凭证种类为“现收”或者“银收”，而其借方会计科目不是现金或银行存款，其他项目正常	检测出来，不予处理，并给出错误信息



• (1) 测试数据法记账凭证输入程序中测试数据法举例

6	记账凭证上凭证种类和会计科目之间的关系	输入一张记账凭证，使其凭证种类为“转账”，而其借方或者贷方出现现金或者银行存款科目，其他项目正常	检测出来，不予处理，并给出错误信息		
7	记账凭证上借贷方平衡关系	输入一张记账凭证，使其借方金额合计与贷方金额合计不等，其他项目正常	检测出来，不予处理，并给出错误信息		
8	记账凭证完全正确时，程序能否通过	输入一张记账凭证，使其各个项目均符合要求	接受		

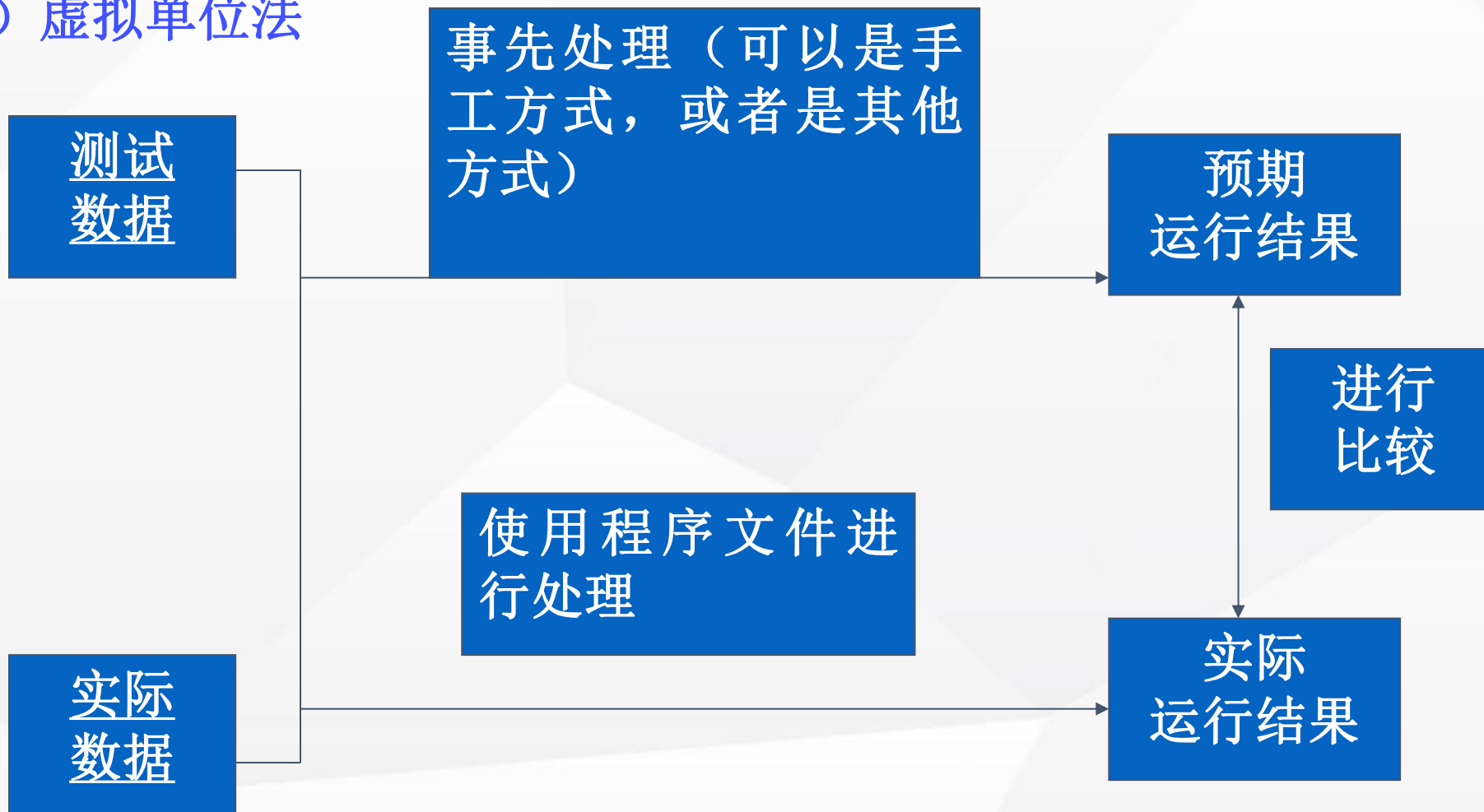




- 二、电算化会计信息系统中程序文件的测试
- （三）运行模拟数据的测试
- 2、具体的测试技术
- （2）虚拟单位法
  - 在虚拟单位法中，审计人员虚拟出一批测试数据，这些测试数据和真实的数据相比较，有一个明显的区别，以后可以将它们分离出来。
  - 这些测试数据和真实数据混同在一起进行实际的运行。
  - 这种方法和测试数据法基本相同，区别在于这里测试数据是和真实的数据混同在一起的。



- (2) 虚拟单位法





- 2、具体的测试技术
- (2) 虚拟单位法
  - 在记账凭证输入程序的虚拟单位测试法中，我们可以和测试数据法一样虚构出一批测试数据，但这里，这些测试数据需要有一个区别于真实数据的地方。
  - 使用虚拟单位法的一个好处是审计人员可以较有把握地认为正在运行和检测的程序就是要审计的程序。
  - 但是，如果将模拟数据直接在实际运行的程序文件上运行，必须妥善地消除模拟数据的影响，否则将引起严重的后果。



- 2、具体的测试技术

- (2) 虚拟单位法

- 消除模拟数据对主文件的影响，基本上可以采用三种方法：
  - 第一种方法是，在设计模拟数据时就将模拟数据和实际数据区分开来，使两者具有比较明显的区别。
  - 第二种方法是，将模拟数据对主文件的影响用反向分录的方法予以冲销。
  - 第三种方法是，先对主文件进行备份，然后，在模拟数据和实际数据混同输入和处理的这个时期，停止实际业务的处理，待模拟数据和实际数据混同处理结束后，重新用备份的主文件恢复，这时再进行实际数据的处理。



# 数据文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 一、电算化会计信息系统中的数据文件
- 会计信息系统中的数据文件分为三大类：
  - 第一类是账务数据库文件
  - 第二类是辅助性数据库文件
  - 第三类是临时工作文件



- 二、电算化会计信息系统中数据文件的测试
- （一）不运行数据文件的测试方法
- 不将数据文件通过电算化会计信息系统进行处理，而直接对数据文件进行测试。
- 其实就是指直接对打印出来的数据文件进行分析。



- 二、电算化会计信息系统中数据文件的测试
- （一）不运行数据文件的测试方法
- 采用不运行数据文件的测试方法，成本比较低，耗时较少，易于理解。
- 但是使用这种方法时要注意判断的是：所得到的打印出来的数据文件是否就是被审计企业电算化会计信息系统中实际的数据文件。



# 数据文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、电算化会计信息系统中数据文件的测试
- （一）不运行数据文件的测试方法
- 在进行测试时，要注意
  - 是否所有数据都被记录到账上，是否有数据被遗漏，计算是否正确，如对存货增减业务的处理是否正确；
  - 是否有分类上的错误，如固定资产和存货的分类是否有误等等。
- 很显然，这种测试方法，和手工会计信息系统中的审计方法基本类似。





# 数据文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、电算化会计信息系统中数据文件的测试
- （二）运行实际数据文件的测试方法
- 1、运行实际数据文件
- 运行实际数据文件的测试方法指审计人员将实际数据文件通过电算化系统进行处理，来测试数据本身的正确性和进行分析性复核。
- 通过实际的运行过程来判断数据的正确性。
- 2、优缺点



# 数据文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

- 二、电算化会计信息系统中数据文件的测试
- (二) 运行实际数据文件的测试方法
- 3、具体的测试方法
  - (1) 利用操作系统和实用程序
  - (2) 利用定制的审计程序
  - (3) 利用通用审计软件



- 二、电算化会计信息系统中数据文件的测试
- (三) 运行虚拟数据文件的测试方法
- 1、运行虚拟数据文件
- 审计人员可以通过运行虚拟数据文件来测试系统处理的正确性。
- 和对程序文件的测试不同的是，在这里，审计人员关心的是系统处理的逻辑是否正确，能否得到正确的结果。
- 2、方法的优缺点



- 二、电算化会计信息系统中数据文件的测试
- (三) 运行虚拟数据文件的测试方法
- 3、具体的测试方法
  - (1) 测试数据法
    - 这种测试方法要求构造和处理一批测试数据。
  - (2) 虚拟单位法
    - 虚拟单位法中需要构造一批测试数据，这些测试数据和被审计企业的真实的数据文件一起进行处理。

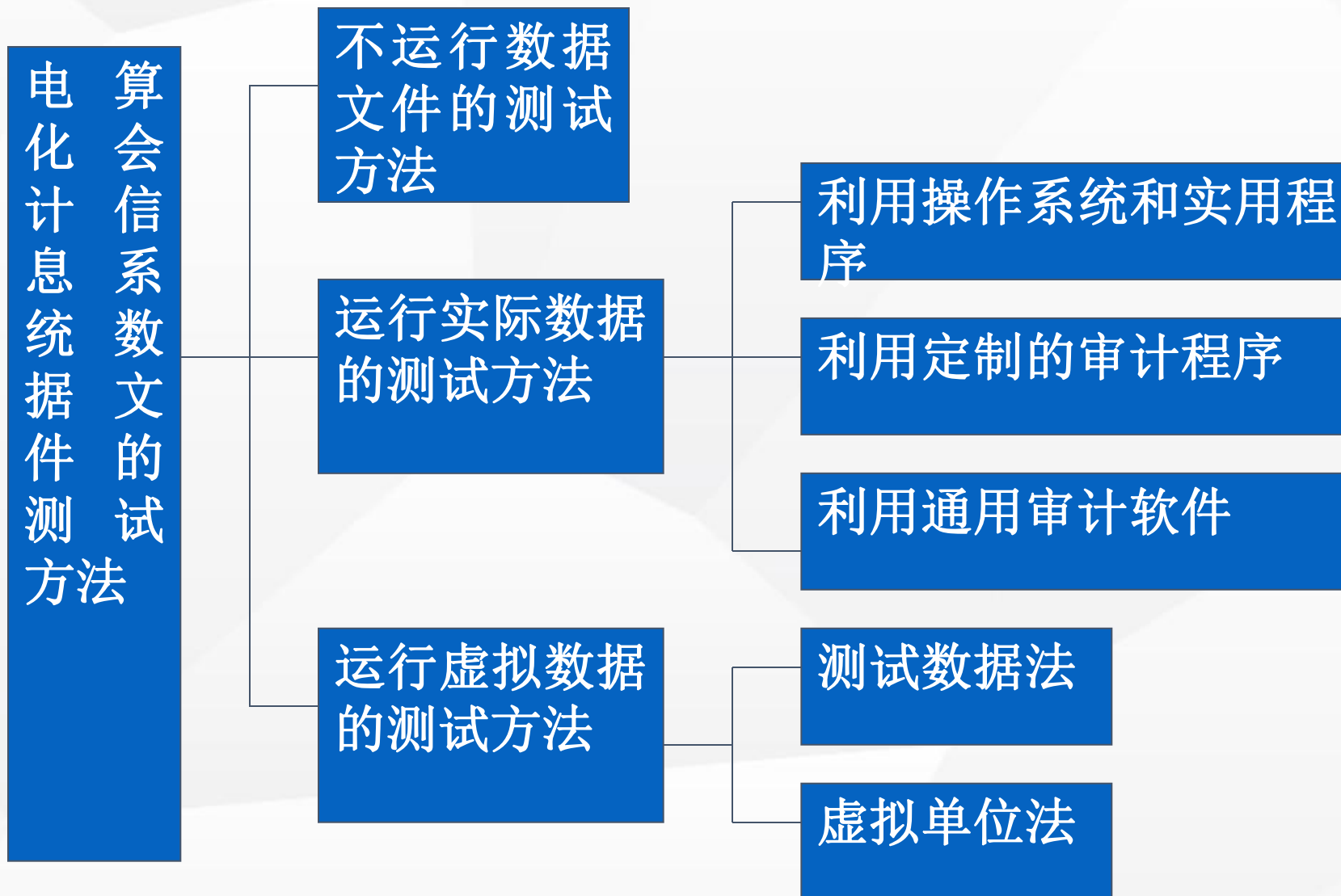




# 数据文件测试



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS





- 会计信息系统审计 的定义
  - 美国信息系统审计的权威专家**Ron Weber**把信息系统审计的定义为“收集证据并对所收集的证据进行评价的一项活动，以决定会计信息系统是否在最经济地使用资源的同时，实现了有效保护资产、维护数据完整、完成组织目标等预期功能。”
  - 信息系统审计是审计行业的一个特殊领域。
  - “未来审计行业和审计技术的发展动力将主要来自于信息系统审计的发展”，这一观点已经逐渐成为国外会计、审计界的一个共识

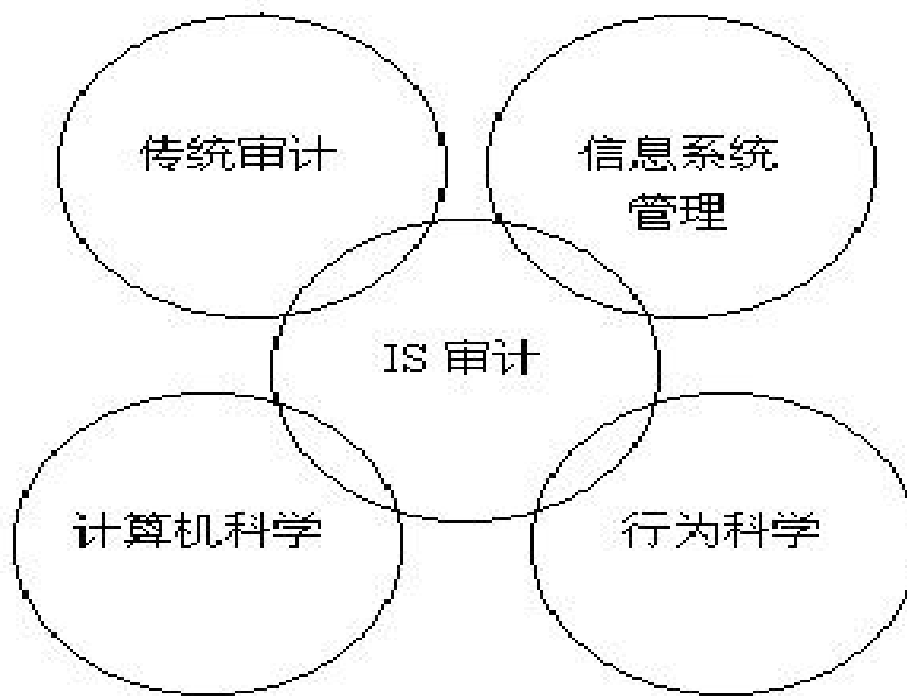


- 会计信息系统审计 的目的
  - 信息系统审计目的是评估并提供反馈、保证及建议，关注的是会计信息系统的可用性、保密性和完整性以及信息系统帮助企业实现目标的效率、效果。
    - **可用性**——商业高度依赖的信息系统能否在任何需要的时刻提供服务？信息系统是否被完好保护以应对各种的损失和灾难？
    - **保密性**——系统保存的信息是否仅对需要这些信息的人开放，而不对其他任何人开放？
    - **完整性**——信息系统提供的信息是否始终保持正确、可信、及时？能否防止未授权的对系统数据和软件的修改？
  - 信息系统审计是保证信息系统质量的行之有效的方法，信息系统审计的定义和目标同样适用于会计信息系统审计。





- 信息系统审计的理论基础
  - 信息系统审计是建立在传统审计理论、信息管理系统理论、行为科学理论、计算机科学等四个理论基础之上的





- 信息系统审计业务范围
- 信息系统审计师必须具备的知识和技能要求
- 信息系统审计的发展
- 我国信息系统审计师的需求市场和供给现状



• 信息系统审计师的知识技能要求



	信息系统方面	实施项目方面
应该具备的背景知识	对财务和管理控制及控制风险的一般了解； 对专业信息系统审计标准应用的全面了解； 对IT相关控制及控制风险的全面了解，主要包括两个方面：IT环境和应用程序/处理； 对操作系统、DBMS和C/S结构的了解； 对信息系统及其设计、部署思想的了解，也包括对审计轨迹影响作用的了解； 对信息系统模块及模块间甚至、集成和部署的了解； 对信息系统安全和授权概念的了解。	对项目管理实务和控制的一般了解； 对IT 领域的项目管理实务和控制的了解； 对IT相关系统开发方法和标准的了解，对变化管理的了解； 对业务过程重组原则和应用程序的了解。
应具备的技能	一个成熟的信息系统审计专业人员应该能够重视信息系统中控制风险的关键领域； 对计算机辅助审计技术及其在信息系统中如何应用的了解； 对所需的额外技能和专业知识（财务和法律方面）的认识能力；	审核评价实施项目的经验



- 信息系统审计技术
  - 审计流程
  - 基于风险的审计方法
  - 审计抽样
    - 统计抽样和非统计抽样
    - 属性抽样和变量抽样



- 计算机辅助审计技术
  - 国际审计准则中的定义
  - 国家审计署的定义
  - 常用计算机辅助审计技术
  - 计算机辅助审计的优点



- ✓ 测试数据生成器
- ✓ 标准工具
- ✓ 软件库程序包
- ✓ 集成测试工具
- ✓ 快照
- ✓ **SCARE/EAM**
- ✓ 审计锚
- ✓ 持续和间歇模拟



- 信息系统审计准则
  - COBIT框架中的《审计指南》
    - 第一层是通用审计方法，包括COBIT框架、审计过程要求、控制目标、通用审计指南等方面；
    - 第二层为过程审计指南及具体审计指南；
    - 第三层内容为实施具体控制目标需要注意的关键环节，包括本地条件、部门特殊标准、行业标准、平台特殊构成、具体控制技术应用。



- **ISACA制定的《信息系统审计准则》**
  - 标准
    - 定义信息系统审计和报告必须满足的最低要求，
    - 目前已经发布的标准
  - 指南
    - 提供了如何应用信息系统准则的具体方法
    - 已生效的**ISACA**信息系统审计指南
  - 程序
    - 提供了信息系统审计师在进行审计任务时的程序范例和如何满足准则要求的信息资料。
    - 给出的程序范例不可能包括所有固有的程序和测试，也不排斥那些能获得相同结果的程序和测试。



- 信息系统审计准则
  - 我国计算机信息系统审计相关法规
    - 1. 审计机关计算机辅助审计办法
    - 2. 独立审计具体准则第20号—计算机信息系统环境下的审计
    - 3. 关于利用计算机信息系统开展审计工作有关问题的通知
    - 4. 中国注册会计师审计准则第1633号——电子商务对财务报表审计的影响
    - 5. 内部审计具体准则第28号—信息系统审计





- 阅读材料：会计信息系统控制损失的策略
  - 会计信息系统面临的风险有哪些？
  - 如何控制会计信息系统面临的风险？



上海财经大学  
SHANGHAI UNIVERSITY OF FINANCE AND ECONOMICS

THANK YOU

