

## 第一章 信息系统审计程序

### ★ 必须的知识点

- 1、ISACA 发布的信息系统审计标准、准则、程序和职业道德规范
- 2、IS 审计实务和技术
- 3、收集信息和保存证据的技术(如观察、调查问卷、谈话、计算机辅助审计技术、电子介质)
- 4、证据的生命周期(如证据的收集、保护和证据之间的相关性)
- 5、与信息系统相关的控制目标和控制(如 Cobit 模型)
- 6、审计过程中的风险评估
- 7、审计计划和管理技术
- 8、报告和沟通技术(如推进、商谈、解决冲突)
- 9、控制自我评估(CSA)
- 10、持续审计技术(即:连续审计技术)

### ★ 可能的考试重点

ISACA 审计标准的变化: 违规和非法行为、IT 治理、在审计计划中运用风险评估

ISACA 审计指南索引与审计程序索引 (不重要)

COBIT (了解和补充)

审计程序 (必考内容)

舞弊检查 (审计师的职业谨慎、内部控制和舞弊)

面谈并观察员工履行职责情况 (审计师识别职能、实际过程、安全意识和报告关系, 原第二章内容)

补偿控制与审计发现的重要性水平 (重要)

审计报告 (一般不会问到格式, 考虑沟通技巧和报告关系)

控制自我评估: CSA 混合方式、CSA 优缺点、审计师在 CSA 中的作用

信息系统审计程序的新变化: 电子底稿、综合审计、连续审计与在线审计

### ★ 知识点摘要

#### 审计章程

信息系统审计(简称:IS 审计, 下同)职能的角色应该建立在审计章程的基础上。一般, IS 审计是内部审计的一部分;因此, 审计章程还包括其他的审计职能。**审计章程应当清楚地说明管理层对于审计职能的责任、目标和委托授权。**审计章程还应全局性地说明审计职能的授权、业务范围和责任。最高管理层和审计委员会, 应当批准这部章程。一旦创立, **就只有在非常必要、并经过充分的论证后才允许变更审计章程。**IsACA 信息系统审计标准要求审计章程或业务委托书上**适当地**描述信息系统审计职能的责任、授权和义务。

#### 对审计师技能的要求

IS 审计师是有限的资源, IS 技术又日新月异地飞速发展。于是, IS 审计师通过不断更新技能通过培训直接获得新的审计技术等方式, 保持其执业资格是非常重要的。尤其, I 审计师

应当懂得管理由经过适当培训的审计员工组成的审计项目团队的管理技术。**IS 信息系统审计标准要求 IS 审计师在技术上胜任、具备执行审计工作所需的技能和知识。**此外，I 审计师可以通过适当的**继续职业教育**保持其胜任性。在制定审计计划和向员工指派审计工作作时，知识和技能要纳入考虑。

**IS 审计管理层也应当提供必要的 IT 资源，以改善 I 审计的熟练能力，例如：提供必要的软件、网络入侵测试之用的扫描器和穿透测试环境。**

## 审计计划

至少每年都应**对短期计划与长期计划**进行分析，特别是在采用了新的技术、新的控制措施及新的评测技术时要做这样的分析得到管理层和审计委员会的批准并根据分析的结果来规划将要开展的审计活动。审计计划应当如果可能的话，尽星通报到各级管理层负责人。

制定审计计划时，I 审计师必须了解执业的整体环境。它包括对审计课题相关的各种业务实务和职能的一般性了解熟悉不同得业务运营环境也包括支持这些活动的各种信息系统和技术。

Is 审计师制定审计计划时，要考虑到审计范围相关的审计对象的目标其技术框架。如果需要，I 审计师也应该**考虑被检查的方面和它与组织的关系(战略的、财务的和/或运营的)**，并获得包括 Is 战略规划在内的战略计划的信息。Is 审计师应该了解审计对象的信息框架和技术方向，来设计适用于审计对象的当前和未来技术的审计计划。

IS 审计计划中，考虑法律、法规的影响。**一是规范审计或信息系统审计活动的法律规则；另一个是与审计委托人的信息系统、数据管理及财务报告等方面相关的法律法规**，后者无论是在内部审计还是在外部审计方面都很重要，组织中任何违反法律法规的事项都将对组织的业务运营有负面影响。

组织中最好能设置法律部门，当发生有关法律方面事务时，Is 控制专员可以得到法律支持。由于不断暴露的财务丑闻，提供给投资者的信息质量变成世界关注的焦点。

## 信息系统审计准则

信息系统审计准则是由信息系统审计准则、审计指南和审计程序构成的。

第一层次:信息系统审计准则。信息系统审计准则是整个审计准则体系的总纲，是信息系统审计师的资格条件、执业行为的基本规范，是制定审计指南和审计程序的基础依据。分为 8 大类，共 12 条准则。只要是信息系统审计师执行审计业务，出具审计报告，都必须遵守执行，具有强制性。

第二层次:信息系统审计指南。审计指南是依据审计准则制定的，是审计准则的具体化，它详细规定了信息系统审计师执行各项审计业务、出具审计报告的具体指南，为审计师在执行审计业务中如何遵守审计准则提供指导。**审计师在执业时运用这些指南，离不开职业判断，对任何偏离指南的行为一定要有充分的理由。**

第三层次:信息系统审计程序。信息系统审计程序是依据审计准则和审计指南制定的。它为**审计师提供了一般审计业务的程序和步骤**，是遵守审计准则和审计指南的一些通用审计程序。审计程序为审计师提供了很好的上作范例。但这仅是审计师的一个参照而已，它所提供的只是审计师在审计时能满足审计准则要求的通常做法，它并不要求强制执行。**审计师在执行具体的审计业务时，要根据特定的信息系统和特定的技术环境做出自己的职业判断，选择适当的审计程序。**

## ISACA 职业道德准则

信息系统审计和控制协会制定了职业道德准则用以指导协会会员和 CII 认证持有者的职业和个人行为。

协会会员和 IS 认证持有者应该遵守以下道德规范:

- 1、遵从并努力符合信息系统审计标准、程序及控制;
- 2、在具体执行审计中要按照职业标准及最佳实践原则要求自己,做到敬业、公正及审慎;
- 3、以诚实及符合法律要求的方式为利益相关者服务,保持高尚的行为及品德,不从事有损于信息系统审计职业的活动;
- 4、对信息系统审计中所取得的信息,应予以保密,不得借以谋取私利和泄漏给他人;
- 5、保持在审计和信息系统控制相关领域的专业胜任能力,有效而可靠地完成审计任务;
- 6、审计结果应向适当的组织、部门和个人报告,并披露所有的重人事项;
- 7、应当对组织中的利益相关者进行信息系统安全与控制的教育,以促进其对审计及信息系统的了解;

## ISACA 信息系统审计标准

审计章程或审计业务约定书应得到组织中适当的管理层的同意和批准。

信息系统审计师在从事审计事项时,应该在实质和形式上独立于被审计方。

信息系统审计人员应编制基于风险的审计方法。

信息系统审计人员应编制详细的**审计计划**,包括**审计性质、目标、范围和所需的资源**。

信息系统审计人员应编制审计程序和步骤。

**在计划和实施审计工作时,信息系统审计人员应该考虑不合规和非法行为等可能带来的审计风险。**

**无论不合规和非法行为的风险评估结果如何,信息系统审计人员在实施审计作业时都要对由于不合规和非法行为而导致的重大误报的可能性保持职业怀疑的态度。**

在确定或得到存在重人的不合规和非法行为的信息时,信息系统审计人员应该及时与**适当的管理层沟通该情况**。

在确定重大的不合规和非法行为牵涉到管理层或和内部控制中关键岗位人员时,信息系统审计人员应该及时与董事会沟通该情况。

如果重大的误报或非法行为影响到信息系统审计人员继续实施审计工作时,信息系统审计人员应该考虑该环境下的法律和职业责任。信息系统审计人员可以采取的行动有:向业务主管人员报告、向公司治理机构或司法机构报告、中止审计业务。

信息系统审计人员应该检查和评估 I 职能部门的使命、愿景、价值观、目标和战略是否与组织相一致。

信息系统审计人员应该检查 I 职能部门是否存在书面明确的业绩标准,评价其履行情况。

## S12 审计重要性 Audit Materiality

### S3 使用外部专家 Use the work of other experts

### S14 审计证据 Audit Evidence

#### 风险分析

风险分析(Risk Analysis)作为审计计划的一部分，它有助于审计师确定信息资产的脆弱性、面临的威胁及由此而产生的风险水平，并根据风险水平来决定如何引入控制措施降低风险。

“风险是特定的威胁利用资产的脆弱性而造成对资产的一种潜在损害，风险的严重程度与资产价值的损害程度及威胁发生的频度成正比”。

信息系统审计人员常常关注高风险问题，如敏感和重要信息的保密性、可用性、完整性以及生成、存储和处理这些信息的重要的信息系统和流程等。在检查这些风险的时候，信息系统审计人员常常评估组织所使用的风险管理过程的有效性。

对实施措施应运用成本效益分析的方法，选择降低风险到管理层可接受的水平的控制措施。审计师在进行风险分析时要考虑以下问题：

比较控制成本与减少风险所得收益

管理层的风险喜好(如，管理层准备接受的剩余风险水平)：

愿意采用的风险降低的方式(如，终止风险、减少发生的可能性、减少影响、转移或保险)

风险评估包括三个过程—风险评估、风险消除和风险再评估。

#### 内部控制

为减少风险所实施的各种政策、步骤、实务和组织结构被称为内部控制。

#### 预防性控制

在事情发生前监测问题监控运营和输入

在问题发生前预测潜在问题，并

做出纠正避免错误、疏忽或蓄意行为的发生

#### 检查性控制

使用控制检查和报告发生的错误、疏漏或蓄意行为的发生

#### 纠正性控制

减少危害影响

修复检查性控制发现的问题

找出问题原因

纠正问题衍生出的错误

修改处理系统以减少未来问题发生的可能性

内部控制设计包括两个重要方面：要达到什么和要避免什么。内部控制不仅作用于业务和运营目标，它还能够预防、检查和纠正不良事件的发生。

## 内部控制目标 IT

保护信息资产

符合组织的方针政策及法律法规的要求

信息输入输出

交易处理的准确性及完整性

数据处理的可靠性

备份与恢复

业务经营的效率与效果

## COBIT

COBIT 控制框架共制定了 34 个高层控制目标，每个目标代表一个 IT 过程，可组合为 4 个领域：计划与组织、采购与实施、交付与支持、监控和评估。通过定位这 34 个高层控制目标，组织可以确保为 IT 环境提供了一个充分的治理和控制系统。

考生应该知道这个框架是什么，做什么用和企业为什么用它

### COBIT 中文手册

## 实施信息系统审计

审计是指有胜任能力的独立机构或人员接受委托或授权，对特定经济实体的可计量的信息证据进行客观地收集和评价，以确定这些信息与既定标准的符合程度，并向利益相关者报告的一个系统过程。

**实施信息系统审计需要如下几个步骤：**

- .充分的审计计划(短期、长期)
- .为有效的利用审计资源，审计机构必须评估所有的风险(一般控制与应用控制领域)
- .制定审计计划，包括审计目标与审计程序
- .收集证据、对现有控制进行评估与测试
- .编写审计报告，并与管理层沟通审计发现

审计管理人员必须确保实施审计的资源和计划是充分可用的。

审计管理人员还应与**管理层**讨论**审计范围、审计目标、原则、步骤、证据、结论意见和结果报告**等。

## 审计程序 ★★

特别要强调的是**审计工作计划**是审计的战略和规划，表明审计的范围和目的，**审计步骤**是为了获取充分、恰当的审计证据来得出和支持审计结论和意见。

**实施审计工作通常包括如下基本步骤： ★★**

- 1、获取并记录对审计对象的了解 **这是进行审计检查的第一步**
- 2、风险评估和总体审计计划和安排
- 3、详细审计计划
- 4、初步检查审计对象
- 5、评估审计对象
- 6、符合性测试，即控制测试
- 7、实质性测试
- 8、报告(或沟通结果)

## 9、后续审计

### 审计方法学 methodology

所谓的审计方法就是通过在组织中制定一系列规范的**审计程序 audit procedures**来达到预期的审计目标，其主要内容包括**审计范围、审计目标及工作程序 APG**。审计方法应当由审计部门的管理人员来制定与批准，

为**测试或检查确定信息来源**，比如：流程图、策略、标准、程序和以往的审计报告

所有的审计规划、计划、测试、发现和相关工作都要记录在**工作底稿**中。底稿的内容应该相关、完整、清晰并被归档保存。

### 舞弊检查

公司治理相关法律法规规定，无论舞弊行为严重与否，**管理层应对舞弊行为负责**，审计人员和审计委员会负责发现和披露舞弊行为。

应有的职业谨慎：审计师应该工作中注意并警惕舞弊行为的发生。

**内部控制并不能完全消除舞弊**，IT 审计师要清楚舞弊行为发生的可能性和舞弊的方式，舞弊行为可能是**利用控制的薄弱环节**，也可能是**通过超越控制**发生的。

在实施常规保证审计任务时，巧审计人员可能会遇到舞弊现象或迹象，经过仔细评估，如果需要进一步的调查，**审计人员**应该将该情况与适当的管理层沟通。一旦审计人员确认发生了**重大舞弊或检查风险很高时**，**审计经理**也应该及时地与审计委员会沟通情况。

### 基于风险的审计 Risk-based auditing 2008 新增

#### 持续审计

Within this concept, inherent risk, control risk or detection risk should not be of major concern, despite some weaknesses. In a risk-based audit approach, IS auditors are not just relying on risk; they also are relying on internal and operational controls as well as knowledge of the company or the business. This type of risk assessment decision can help relate the cost-benefit analysis of the control to the known risk, allowing practical choices.

在了解业务的基础上，对风险进行分类，根据不同业务不同风险设置权重，**首先必须了解业务流程 business process**，**业务的内在风险 inhrent risk**（因为这个风险是和业务的属性相关的）

在采用基于风险的审计方法时，信息系统审计师不仅仅是依赖于对风险的认识，而且还依赖于对组织的**内部控制和运营控制**的分析。这种类型的风险评估就是把风险意识贯穿到审计的全过程，从而在审计过程中把重点放在审计风险的评估上，并有助于把对控制所做的成本效益分析与已知的风险结合起来，作出最佳控制选择。

#### 审计风险可分类如下：我们日常说的审计风险是指检查风险

**固有风险 inherent risk**。是指“假设不存在相关的内部控制的情况’下，发生重人错误的风险”。也可以说，在不存在相关控制时，出现重大错误的敏感度。例如：复杂的计算比简单的计算更有可能出错，现金较存货更可能容易被偷。**固有风险的存在，与审计无关，其发生是由于企业性质所致。有没有制度风险都存在。不存在（无法存在）补偿性控制措施**

**控制风险 control risk**。是指有内部控制制度，但无法预防、及时发现或纠正重要错误的风险。例如，手工检查计算机日志的风险会很高，因为日志信息量太大了，很容易漏掉需要检查的活，而使用计算机数据校验程序的控制风险就会很低。**有控制制度但还是发生，不同**



的制度发生程度不同的风险。

**检查风险 detection risk**。是指信息系统审计人员由于采用了不恰当的测试程序，未能发现已存在的重大错误的风险。在审计工作的风险评估阶段，错误检查不能被确定。但识别检查风险能够更好的评价审计人员的检验、确定并建议纠正重大错误的能力。

**整体审计风险**。整体审计风险是对个别控制目标所评估出的**各类审计风险的综合**。审计的目标即是对审计范围予以缜密审查，以控制其审计风险，以使在完成审计时，将整体审计风险控制到尽可能低的程度；另一目标是尽可能有效地评估并控制风险，以达到所要求的程度。

### 重要性

在制定审计计划时，信息系统审计师要对审计风险有清楚地认识。**审计抽样可能不会检查出全部的潜在错误**，但通过使用恰当的统计抽样程序或质量控制程序，会大大减少检查风险的概率。

在评估内部控制时，信息系统审计师也要认识到既定的检查系统可能不会发现小的错误，但小错误与其他错误组合在一起可能就会对整个系统产生重大影响。**审计检查时不要忽略小错误。**

“重要性”的评估依赖于信息系统审计师的职业判断。信息系统审计师可能发现，一项在业务层认为很重要而高级管理人员却认为是不重要的“小”错误。**了解审计风险并衡量其重要性，是计划审计范围及审计测试应具有的基本观念**。重要性是指对整个组织的全部的潜在影响。

**发现了和检查范围相关的问题，正确的做法是对与当前范围相关的内容重点检查，建议衍生检查可能存在问题的地方。如果在当前项目中延伸可能影响当前时间进度，而且也没有足够的审计资源。**

### 风险评估技术

风险评估的一种常用技术是**评分系统**，对风险因素进行评估，优先审计高风险区域。考虑的风险因素主要有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。审计人员通过比较各变量的风险值，赋予风险变数一定的权值。

另一种技术是**审计师根据专业经验、业务知识、管理层的指导、历史表现、业务目标、环境因素等进行判断**，以决定风险大小及审计的优先级。两种技术结合使用的效果可能会更好。不存在一成不变的风险评估技术

### 信息系统控制目标

信息系统审计师应当能够把这种一般控制目标转化为特定的信息系统控制目标，因为在信息系统审计计划中确定审计目标是非常重要的一步。信息系统审计的基本目的之一就是**确定控制目标及验证当前针对此目标已采取的控制措施是否有效**。

### 符合性测试 compliance testing 与实质性测试 substantive testing

信息系统审计师对识别的关键控制点进行符合性测试，初步**了解各项控制的实施效果**。审计师根据符合性测试的结果确定实质性测试的范围大小及时间长短。

测试组织符合控制程序所收集的**证据与评估交易、数据或其他信息的完整性**所收集的证据是完全不同的。前者称为**符合性测试**，后者称为**实质性测试**。

符合性测试确定控制的执行符合管理层制定的方针政策的程度。**测试既定程序的存在和有效性**。

**实质性测试验证实际处理的完整性**。通过实质性测试可以确定财务报表和财务信息所反映

的业务活动的正确性和完整性。信息系统审计师使用实质性测试测算直接影响财务报表的金额错误。

需要进行实质性测试的数量与内部控制水平直接相关。**如果符合性测试(也叫控制测试)结果表明被审计单位内部控制充分, 信息系统审计师就会减少实质性测试程序。**

## 证据

审计证据包含审计人员的观察、询问的记录、从内部文件或信件中取得的资料、审计测试程序所产生的结果。

**评估审计证据的可靠性**, 取决于以下因素:

**提供审计证据人员的独立性**。审计证据由**外部人员**提供比内部人员提供更可靠, 这也是为何要采用询证函来验证应收账款余额的原因。

**提供审计信息或证据人员的资格(能力)**。不论提供审计信息或证据者是外部或内部人员, 审计师都应考虑提供审计证据人员的资格。对审计师也需作同样的考虑。如果审计师对其所审计的技术领域不能很好地理解, 特别是如果审计人员对测试不完全了解时, 则在测试该领域时所收集的信息可能是不可靠的。

**审计证据的客观性**。客观的审计证据比需要判断或解释的证据好。如财务审计人员清点现金是直接、客观的证据, 而审计师分析应用系统的效率, 是根据与特定人员的讨论结果来确定的, 可能不是客观的审计证据。

**审计证据的时效性**。信息系统审计师应当考虑在进行符合性测试、实质性测试时相关信息的时效性问题。例如, 电子数据交换(EDI)、文档影像处理、电子表格等应用系统对数据的更新如果没有日志记录审计踪迹, 或者文件没有备份, 那么经过一段时间以后, 就无法对以前某一交易发生时的具体时间及当事人进行追踪与审查了。

## 抽样

抽样是应用在成本及时间都不允许对所有交易或事件的对象总体作 100%的审计时, 可以从审计总体中选取一定数量的样本进行测试, 并根据测试结果, 推断审计对象总体特征的一种方法。审计抽样分类的方法有很多种, 常用的分类方法是:按抽样决策的依据不同, 将审计抽样分为统计抽样和非统计抽样;按审计抽样所了解的总体特征的不同, 将审计抽样分为属性抽样和变量抽样。

不论是**统计抽样**或**非统计抽样**在确定总体特性时都需要审计人员运用职业判断, 因而存在得出错误结论的风险(抽样风险)。

**属性抽样和变量抽样:**

属性抽样。估计一个控制或一组相关控制属性的发生概率。例如, 使用电脑中请表中的核准签名就是一种控制属性。属性抽样主要是用来测试控制的, 与**符合性测试**相关。

**固定样本量抽样** (先确定样本量 它是最为广泛使用的属性抽样技术。)

**停一走抽样** 它从预计总体误差为零开始, 通过边抽样边审查评价来完成抽样审计工作。

**发现抽样** 只要样本中有一个发生数, 就足以形成对总体的统计结论, (发生问题的比例较大的情况下 总是能抽出一个偏差样本)

变量抽样:根据总体的抽样来估计总体的金额数或其他衡量单位, 如重量。。变量抽样与**实质性测试**相关, 其主要目的是验证可能存在于程序或功能中的因控制失效导致重大影响的最人金额。例如, 检查一个公司重大交易的资产负债表, 并对生成资产负债表交易结果的程序进行检查。

**分层单位平均估计抽样** 先对样本总体进行分层, 在不同分层中进行抽样检查确定样本



的平均值，

不分层单位平均估计抽样 通过抽样检查确定样本的平均值，根据样本平均值推断总体的平均值和总值的方法。

差额估计抽样 差额估计抽样是以样本实际价值与账面价值的平均差额来估计总体实际价值与账面价值的平均差额，然后再以这个平均差额乘以总体项目个数，从而求出总体的实际价值与账面价值差额的一种抽样方法。

**精度值越大，样本量就越小，总体误差值就越大：**

执行审计抽样测试的主要步骤包括：

- .决定测试的目标；
- .定义抽样的总体；
- .决定抽样的方法，如变量抽样或属性抽样。
- .计算样本大小；
- .选择样本
- .评估样本

：

**利用其它审计人员或专家进行审计 2008 新增**

### 计算机辅助审计技术

整体测试(Integrated test facility)—在软件系统内置入虚构实体，并以测试资料或正式资料，针对该实体进行处理，以验证其正确性。但其缺点是测试数据可能会进入被审计单位的真实数据环境。

系统控制审计审核文档(Scarf)—在应用系统内嵌入审计软件，以便对系统交易进行持续性的监视，这些资料被存入一个特殊电脑文档，以便让审计师检查。

**比较广泛并一致的审计范围；**

**更有机会量化内部控制的弱点；**

### 审计证据评价

进行信息系统审计时，审计师可能发现一些健全的控制以及控制缺陷。在评估整体控制结构时，信息系统审计师要考虑到，在某些情况下，**一个健全的控制其他地方可能补偿另一个控制的缺陷**。这些在证据评价过程中都需要被考虑。例如，即使审计师发现系统交易异常报表有缺陷，但以详细的人工程序结算所有交易，可补偿这一控制缺陷。审计师应在发现控制缺陷时，了解是否有**补偿性控制**。

**审计师应在报告控制缺陷之前，先审计补偿性控制。**

### 审计报告

信息系统审计师应在报告发布之前，就重要发现及时和合适的人员进行交流，但**提前交流不应该改变报告的内容**：

确保所推荐的改进措施是可行的并**符合成本效益原则**，否则可通过协商方式找出替代方法，并制订出执行日期。

**审计文档应当支持审计发现与审计结论。审计证据的时效性**在支持审计发现与审计结论时是

### **控制自我评估 Control self-assessment**

控制自我评估(CSA)可以被认为是一种**管理技术**，它可以使股东、消费者和其他有关方确信公司内部控制系统是可靠的。它也能保证**员工意识到**公司所面临的风险并主动实行定期的控制检查。用来对关键业务目标、实现目标所面临的风险及管理业务风险的内部控制进行检查的一系列正式的、程序化的过程。

**CSA 的目标包括对直线管理者在控制职责、监督和专注于高风险领域的训练。**加强审计责任。高级管理层能够做出内部控制充分性的保证，满足各法律机构和法规

实施 CSA 方法有几个目标。主要目标是通过把一些控制监督的功能分散到职能部门，以发挥内部控制的**优势**。这并不是削弱审计的功能，反而在**某种程度上增强了审计的功能**。通过明确基层管理人员不仅要对其工作环境的控制负责，而且要**监督控制的有效性**，这样做的好处是各种控制措施落实到具体的业务流程中去。cSA 方法还要教育管理人员如何针对风险区域设计控制方法与监督措施，CSA 方法不仅仅是作为策略来要求员工遵守，**还要求员工参与到 CSA 的设计与执行中来，因为只有基层的员工才最清楚业务流程及其薄弱点所在。**

如果在 CSA 项目中包括了审计师，**审计师应当作为内部控制专家及评估推动者的角色**而出现。CSA 中审计师的价值在于促进管理人员在他们的授权管理范围内承担了内部控制的责任及明确了所有者身份，使管理人员对控制结构进行流程改善并落实监督工作责任。

### **持续审计（连续审计）**

连续监控—它是一种 IS 管理工具，一般基于自动化程序，来达到预定监督要求。例如，实时防病毒或入侵监测系统就是以连续监控的方式运行的。

连续审计—它是独立审计师对审计对象**提供书面保证**的一种方法，它是在审计对象发生事件的同时，或在短时之后，发表的一系列审计师报告。连续 Is 审计(或非 I 审计)一般都使用自动化的审计程序。

### **英文版书的题目**

1-8 制定审计计划的第一步是要了解组织的业务、目标

1-9 确定审计范围的依据 risk risk-based

1-10 磁带数据备份是一种典型的 correction control **纠正性控制**