CISA 简介

- 唐龙
- CISA

CISA overview

- CISA and ISACA
- CISA认证
- CISA考试
- CISA考试内容
- CISA vs. CISSP
- 信息审计过程

CISA and ISACA

CISA and ISACA

- CISA
  - Certified Information System Auditor
  - 注册信息系统审计师

- ISACA
  - Information Systems Audit and Control Association
  - 信息系统审计与控制协会

ISACA

- 信息系统审计与控制协会（ISACA）创始于1967年，当时它是由从事同类职业的人所组成的小团体——计算机系统的审计和控制对他们各自机构的运作都变得愈发关键——因此他们聚集起来讨论制定信息集中化资源和本领域指导准则的必要性。在1969年，这个团体正式组建为EDP 审计师协会。在1976年，这个协会成立一项教育基金来开展大规模的研究工作，以拓展信息产业管理与控制领域的知识与价值。

ISACA

- 今天，ISACA在全球有四万多名成员，他们的组成非常具有多元性。这些成员在100多个国家内生活和工作，并涵盖众多专业信息技术的相关职业，比如信息系统审计师、顾问、教导员、信息系统安全专家、管理者、首席信息官和内部审计师等。有些职业是本领域内新兴的，其他为中级管理人员，另外还有许多人担任最高级的职位。他们几乎遍及所有行业，包括财政金融、公共会计、政府与公共部门、公用事业和制造业。这种多元性使众多成员能够相互学习，并在许多专业问题上广泛交流彼此的观点。该特点一直被认为是ISACA的强势之一。

ISACA

- ISACA的另一个强势就是它的分会网络。ISACA的分会遍布世界60 多个国家，可提供成员教育、资源共享、支持、专业网络，以及其他由当地分会提供的诸多利益。

ISACA

- 在ISACA创立的三十年来，它已成为一个为信息管理、控制、安全和审计专业设定规范的全球性组织。
- 它的信息系统审计和信息系统控制标准为全球执业者所遵从。它的研究工作针对那些挑战其重要原则的疑难专业事项。
- 它的国际信息系统审计师（CISA）认证得到全球的公认，并有三万多名专业人员得到认证。
- 它最新推出的国际信息安全经理（CISM）认证特别针对信息安全管理的审计事务。
- 它出版了领先于信息控制领域的技术性期刊，即《信息系统控制期刊》（*Information Systems Control Journal*）。
- 它举办一系列国际性会议，并且把焦点集中于信息系统保障、控制、安全和信息技术管理专业的技术与管理主题上。

ISACA

- 唯一有权授予信息系统审计师资格的跨国界、跨行业专业机构

ISACA Web

- http://www.isaca.org

CISA认证

CISA的工作

- 熟悉信息系统软件、硬件、开发、运营、维护、管理以及安全
- 熟悉业务运营管理
- 利用规范和相关的审计技术，对信息系统的安全性、稳定性、有效性进行审计、检查、评价

CISA证书的价值

“全球化进展进一步提升了*CISA*资格证书的价值，显示了它是真正国际认可的资历证书。”

---------美国摩根大通公司，埃内斯托·阿吉拉，CISA

CISA证书的价值

- 专业认证计划杰出的标志在于持证人提高了自身的价值并受到了人们的尊重。自1978年以来，由信息系统审计与控制协会（ISACA）发起的国际信息系统审计师（CISA）认证已经成为持证人在信息系统审计、控制与安全等专业领域中取得成绩的象征，并逐步发展成全球公认的标准。

最高专业程度的标志

- 获得CISA资格证书有助于确立您作为一名合格的信息系统审计、控制和安全专业人才的声望。不论你是希望提高你的工作业绩还是得到职务升迁，拥有CISA资格证书都会使你拥有他人无法企及的竞争优势。

雇主寻求的资历

- 由于CISA 所认证的个人能够熟练掌握当今需要的最先进的技能，雇主更愿意雇用和留住那些达到并能够维持资格证书所要求水平的人才。CISA资格证书向雇主保证其雇员已达到工作要求所必需的最新教育与实践经验。

- “*CISA* 用它的四个字母向未来雇主表明：

我具备扎实的信息系统审计知识与丰富的经验。*CISA* 使持证人在市场中占据优势。”

---------英国苏格兰皇家银行，罗勃特·科里斯，CISA

全球的认可

- 也许本认证对于你当前的工作并不是绝对必需的，然而越来越多的机构希望员工得到CISA认证。为了确保你在全球市场中的成功，选择一个建立在全球认可技术实务基础上的认证是至关重要的。CISA所提供的就是这种认证。CISA作为信息系统审计、控制与安全专业人员的资格证书，受到全世界所有行业的广泛认可。

得到ISO/IEC 17024:2003标准的公认

- 美国国家标准协会（ANSI）已经按照ISO/IEC 17024:2003标准对CISA认证计划进行了鉴证和认可
- 该标准是对一个团体开展人员认证方面的总体要求

成为CISA

- 顺利通过CISA的考试；
- 遵守国际信息系统审计与控制协会的『职业道德准则』
- 提供从事信息系统审计、控制与安全工作5年以上经验的证明。具有下列同等经验，可申请免除该项经验，并应获得如下证明：
- 1 年以下的信息系统审计、控制与安全工作的经验可用如下资历相抵：
  - 满1 年的非信息系统审计工作经验，或
  - 满1 年的信息系统工作经验，和 / 或
  - 具有大专学历（大学60 个学分或同等学历）。
- 2 年信息系统审计、控制与安全工作的经验可用学士学位（大学120 个学分或同等学历）相抵。
- 1 年信息系统审计、控制与安全工作的经验可用2 年相关领域（计算机科学、会计、信息系统审计等）内从事大学专职讲师的经验相抵。无最高年限（即6 年大学讲师经验等同于3 年信息系统审计、控制与安全工作的经验）。

成为CISA

- 专业经验必须在申请前的10 年之内获得，或在第一次通过考试之日的前5 年之内。认证申请必须在通过CISA考试的5 年之内提出。所有专业经验都必须由原雇主独立地确认。

CISA考试

CISA考试

- CISA考试在每年6 月份和12月份举行
- 考题包含200 道多项选择题
- 考试时间为4 个小时
- 450分通过,总共800分

考试报名

- 填写并邮寄报名表
- 线上报名

- 报名费：$510
- 每年8月16日之前：$460
- 线上报名：可节省$35

考分的邮寄

- 自考试之日起约6 个星期后，考生将接到邮寄的考试成绩通知。为了对考试分数保密，考试结果将不采用电话、传真或电子邮件的方式进行通知。然而，如果你在报名表的第27项上表明同意，我们可以通过电子邮件向你发送及格/不及格的考分。

CISA 资格证书的维持

- 获得任何职业资格证书的持证人必须参与继续教育计划来维持其资格证书。为了维持CISA资格证书，持证人必须履行继续职业教育政策，并遵守ISACA协会的『职业道德准则』。这些计划有助于保证CISA 持证人能够与业内先进技术的发展保持同步，并展示较高的职业原则。
- 『继续职业教育政策』要求持证人获得并提供最低限度的继续职业教育（CPE）学时，并每年支付维持费。此外，最低学时的获得与提供必须在固定的3 年认证期内完成。不能履行此政策的持证人拥有的认证资格将被撤消。

CISA考试内容

CISA Content Areas Effective 2011

- 1 信息系统审计程序 14 %
- 2 IT治理与管理 14%
- 3 信息系统获取开发和实施 19%
- 4 信息系统运行、维护和支持 23%
- 5 信息资产保护 30%

第一部分 信息系统审计程序

- 1.1 ISACA 发布的信息系统审计标准、准则、程序和职业道德规范
- 1.2 IS 审计实务和技术
- 1.3 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）
- 1.4 证据的生命周期（如证据的收集、保护和证据之间的相关性）
- 1.5 与信息系统相关的控制目标和控制（如CobiT 模型）
- 1.6 审计过程中的风险评估
- 1.7 审计计划和管理技术
- 1.8 报告和沟通技术（如推进、商谈、解决冲突）
- 1.9 控制自我评估（CSA）
- 1.10 不间断审计技术(即：连续审计技术)

第二部分 IT 治理(信息技术治理)

- 2.1 IT 战略、政策、标准和程序对于组织的意义，及其基本要素
- 2.2 IT 治理框架(体系)
- 2.3 制定、实施和维护IT 战略、政策、标准和程序的流程。如：信息资产的保护、业务持续和灾难恢复、系统和基础建设生命周期、IT 服务交付与支持
- 2.4 质量管理战略和政策
- 2.5 与IT 使用和管理相关的组织结构、角色和职责。
- 2.6 公认的国际IT 标准和准则(指导)。
- 2.7 制订长期战略方向的企业所需的IT 体系及其内容
- 2.8 风险管理方法和工具
- 2.9 控制框架(模型)的使用，如：CobiT、COSO、ISO 17799 等控制模型。
- 2.10 成熟度和流程改进模型(如：CMM、CobiT)的使用。

第二部分 IT 治理与管理

- 2.11 签约战略、程序和合同管理实务。
- 2.12 IT 绩效的监督和报告实务
- 2.13 有关的法律、规章等问题(如：保密法/隐私法、知识产权、公司治理的要求)
- 2.14 IT 人力资源管理
- 2.15 IT 资源投资和配置实务(如：投资的资产管理回报)

第二部分 IT 治理与管理

- 2.16 数据备份、存储、维护、保留和恢复流程，和实务。
- 2.17 业务连续性和灾难恢复有关的法律、规章、协议和保险问题。
- 2.18 业务影响分析(BIA)
- 2.20 开发和维护灾难恢复和业务连续性计划。
- 2.21灾难恢复和业务连续性计划测试途径和方法
- 2.22 与灾难恢复和业务连续性计划有关的人力资源管理。例如：疏散计划、(紧急)响应团队。
- 2.23 启用灾难恢复和业务连续性计划的程序(或流程)。
- 2.24 备用业务处理站点(指场所和设施)的类型，和监督有关协议/合同的方法。

第三部分信息系统获取、开发与实施

- KS3.1 收益管理实践（例如可行性研究，业务模式，总体拥有成本，投
- 资回报率）。
- • KS3.2 项目治理机制（例如项目操控委员会，项目指导委员会，项目管
- 理办公室）
- • KS3.3 项目管理控制框架，管理实务和工具
- • KS3.4 与项目有关的风险管理实务
- • KS 3.5 与数据、应用及技术相关的IT架构模型（分布式应用、基于Web的应用、Web服务、N层应用）
- • KS 3.6 信息系统获取实务（例如供应商评估，供应商管理）
- • KS 3.7 需求分析和管理实务（需求验证，可跟踪性和差距分析，脆弱
- 性管理，安全需求）

第三部分 信息系统获取、开发与实施

- KS 3.8 项目成功的标准与风险
- • KS 3.9 在信息系统中保证交易及数据的完整性、准确性、合法性及适
- 当授权的控制目标和相关技术
- • KS 3.10 信息系统开发方法和工具，及对其优缺点的理解（例如：敏捷
- 开发法、原型法、快速应用开发、面向对象的设计方法）
- • KS 3.11 与信息系统开发相关测试方法与实践
- • KS 3.12 与信息系统开发相关的配置管理与发布管理
- • KS 3.13 信息系统迁移和基础设施部署实务，以及数据转换工具，技术
- 和程序
- • KS 3.14 信息系统实施后审核的目标与方法（例如项目收尾，控制实施
- ，效益总结，绩效测量）

第四部分信息系统运行、维护和支持

- KS4.1 服务水平管理实务及服务水平的组成内容
- • KS4.2 监控第三方与组织的内部控制指标符合性的技术
- • KS4.3 操作与最终用户程序，用来管理计划与非计划的活动
- • KS 4.4 硬件、网络组建、系统软件与数据库管理系统相关的技术概念
- • KS 4.5 确保系统接口整合的控制技术
- • KS 4.6软件许可及软件库存目录管理实务
- • KS 4.7系统容错工具及技术（例如：容错硬件与软件、单点故障消除设
- 备、集群）
- • KS 4.8数据库管理实务；
- • KS 4.9 IT能力计划和对能力进行监督的工具与技术
- • KS 4.10系统绩效监督的过程、工具和技术（例如：网络分析、系统利
- 用率报告、负载平衡）

第四部分信息系统运行、维护和支持

- KS 4.11事件管理、问题管理实务（例如：帮助台、事件升级程序、服
- 务追踪）
- • KS 4.12管理计划变更及紧急变更的过程，包括对生产系统和基础设施
- 的更改、配置、发布及修补等实务
- • KS4.13 数据备份、存储、维护、保存和恢复实践的知识
- • KS4.14灾难恢复相关的法律、法规、合同和保险相关的知识
- • KS4.15与灾难恢复计划相关的业务影响分析（BIA）知识
- • KS4.14用于启动业务连续性计划的人力资源管理实践方面的知识
- • KS4.16灾难恢复计划开发与维护的知识。
- • KS4.17备用处理站点的类型和用来监视合同条款的方法（如热站、温站
- 、冷站）。
- • KS4.18 用于启动灾难恢复计划流程方面的知识。
- KS4 19 灾难恢复演练方法的知识

第五部分 信息资产保护

- KS5.1设计、实施和监控安全控制的技术，包括安全意识；
- • KS5.2对安全事件监控与响应的流程（例如：事件升级程序、紧急事件
- 响应团队）；
- • KS5.3对用户访问授权的系统功能和数据的行为进行识别、认证及限制
- 的逻辑访问控制技术；
- • KS5.4软硬件（例如：应用、操作系统）和数据库管理系统的安全控制
- • KS5.5虚拟化的风险和控制；
- • KS5.6网络安全控制的配置、实施、操作和维护；
- • KS5.7网络和Internet安全设备、协议和技术；
- • KS5.8信息系统攻击方法和技术；
- • KS5.9检测工具和控制技术（例如：恶意软件、病毒检测、间谍软件）
- • KS5.10安全测试和评估工具（例如：渗透测试、脆弱性扫描）；

第五部分 信息资产的保护

- KS5.11数据泄露的风险和控制；
- • KS5.12加密技术；
- • KS5.13公钥基础设施（PKI）和数字签名技术；
- • KS5.14对等计算、即时通信、基于web的技术(例如：社交网络、留言板
- ，博客)等相关的风险和控制；
- • KS5.15与使用移动和无线设备相关的控制与风险；
- • KS5.16语音通讯安全（例如：PBX，VoIP）；
- • KS5.17证据保全技术和过程以及调查取证（如IT过程，证据链）；
- • KS5.18数据分类、分级标准和支持策略；
- • KS5.19物理访问控制鉴别、认证、授权机制；
- • KS5.20环境保护设施以及支持细则；
- • KS5.21存储、检索、传送和处置机密信息资产的过程与程序。

CISA vs. CISSP

认证侧重点

- CISSP
  - 信息系统安全的管理与实践
- CISA
  - 信息系统的控制与审计

对应的职业不同

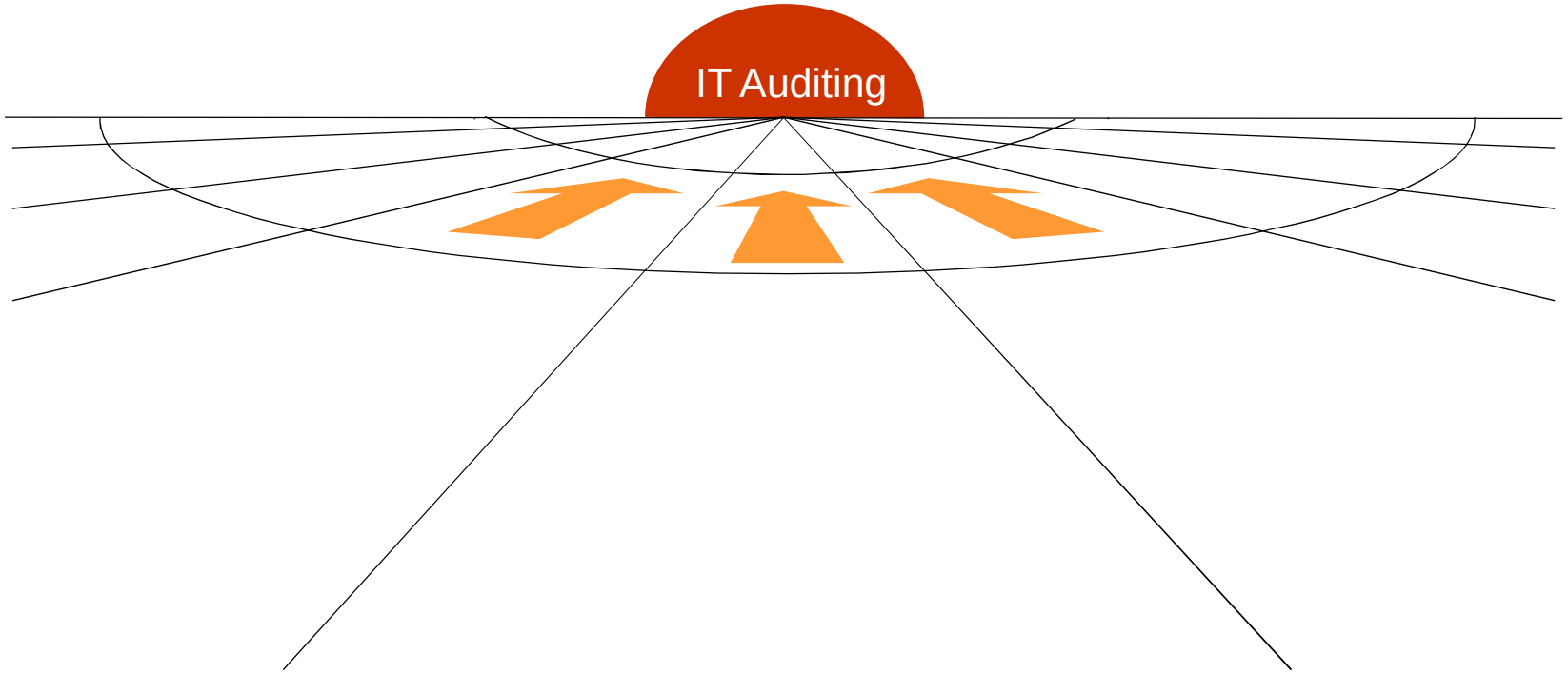
- CISSP
  - Consultant, management
- CISA
  - Auditor, management

考试难度比较

- 技术深度
  - CISSP〉CISA
  - CISSP　　10 domains
  - CISA　　6 domains

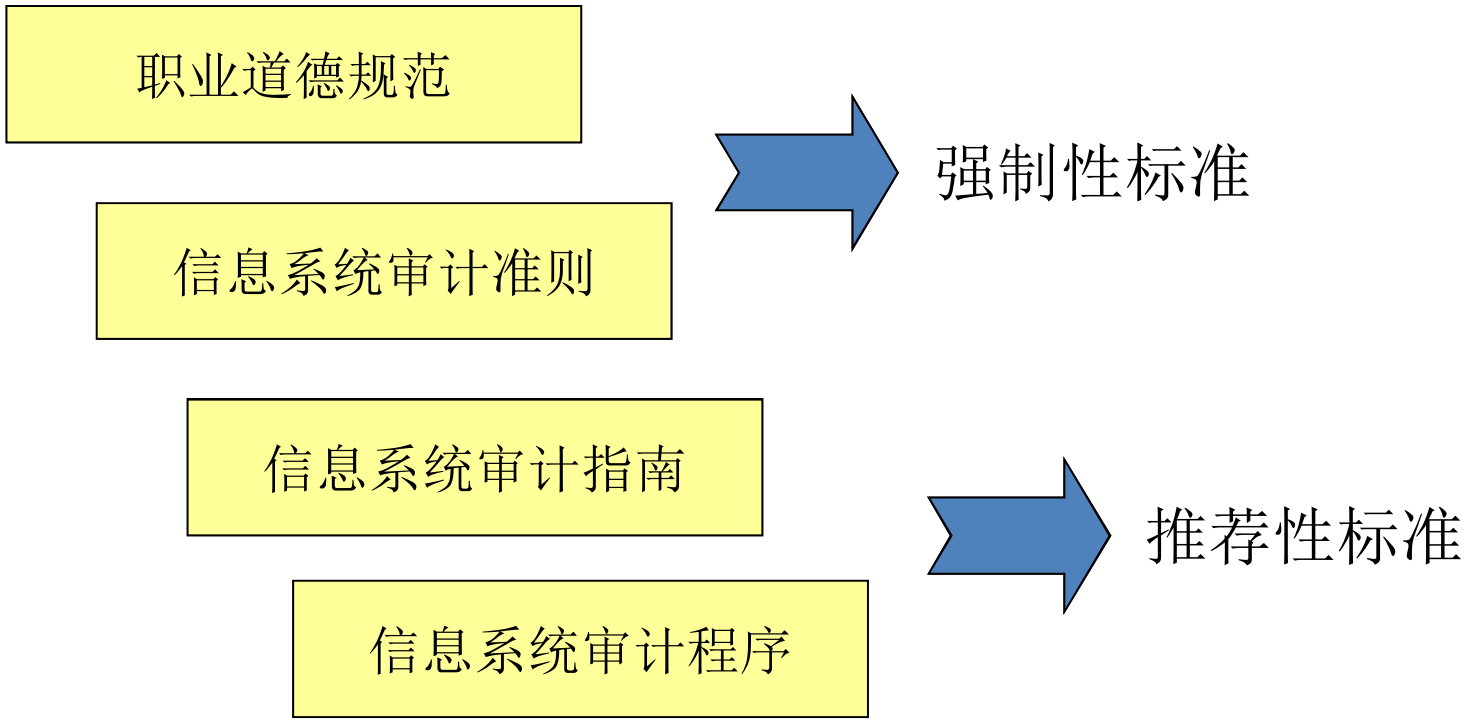
- 答题压力
  - CISA〉CISSP
  - CISSP　6小时　　250题
  - CISA　4小时　　200题

信息系统审计过程



信息系统审计准则与指南

- 提高信息系统审计质量、促进审计从业人员之间的经验交流，促进审计职业的良好发展



- IT审计职业道德规范
  - 职业道德规范(Code of Professional Ethics)

u 信息系统审计师应在审计工作中自觉严格遵循相关实施准则、程序及控制，并遵守相关法律法规的要求；
u 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。
u 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；
u 对信息系统审计过程中所取得的信息，应予以保密，不得借以谋取私利和泄漏给他人。执法机构的司法调查除外；
u 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；
u 应获得充分及适当的证据，作出审计结论及建议，审计结果应向适当的组织、部门和个人报告；
u 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；

  - 职业审慎(Due Professional Care)

u 指工作勤勉程度和开展工作所必需的技能要求，体现在信息系统审计师的职业判断过程中，是确保客户获得高质量审计的基础

- 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。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
  - ISACA标准委员会制定了11大类信息系统审计准则。
- 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。指南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。
  - 审计师在运用这些指南时，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。
  - ISACA标准委员会制定了35条信息系统审计指南。

- 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常审计程序；
  - 审计程序为审计师提供了很好的工作范例，但审计师在执行具体的审计业务时，还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。

3.2 信息系统审计方法

- 审计章程 (Audit Charter)
  - 组织通过审计章程来确定信息系统审计活动在组织中所扮演的角色。
  - 审计章程既要强调管理层本身的对信息系统审计的责任与目标，以及对信息系统审计的授权，也要明确信息系统审计师可以行使的权力、所负责任及审计范围。

一般性审计方法	
审计对象	▪ 确定审计对象
审计目标	▪ 确定审计目标，如：审计目标是确定对程序源代码的变更是否有良好的定义和控制。
审计范围	▪ 确定特定的系统、功能或组织单元进行审核。例如，在程序源代码变更管理审计中，可以把范围限制在某一个应用系统中，或在一个有限的时间范围内。
审计资源	▪ 确定进行审计的地点及设施
审计方案	▪ 确定和收集证据的方法来验证和测试控制 ▪ 确定访谈对象 ▪ 确定和收集组织的相关政策、标准和指南进行检查
实施审计	▪ 以走访、面谈、测试、分析、复核等方法收据审计证据。
评价测试检查结果	（因组织不同而变化）
与管理人员沟通	（因组织不同而变化）
准备审计报告	▪ 确定后续检查方法 ▪ 确定评价与测试审计对象运营的效率与效果的方法 ▪ 确定测试控制的方法 ▪ 检查和评价文档、政策及程序的完备性

- 审计方法(Audit 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方法来达到预期的审计目标，也可称为审计策略。
  - 主要内容包括审计范围、审计目标及工作程序。
  - 审计方法论应当由审计部门的管理人员来制定与批准，并在审计人员中推广应用。

- 审计计划(Audit Plan)
  - 短期计划－本年度内需要实施的审计事项
  - 中长期计划－2年以上的审计计划
  - 制定审计计划的要点：

u 充分了解组织的业务目标、业务流程及信息技术
u 进行风险评估、实施内部控制检查
u 确定审计范围及目标、制定审计方案及审计策略
u 审计计划应当得到管理层和审计委员会的批准，如果可能的话，尽量通报到各管理层负责人
u 综合考虑审计项目要求、人力资源现状及其他限制条件，合理匹配审计资源

- **审计资源管理**
  - 审计师的信息系统相关知识与能力
  - 审计项目管理的能力
  - 审计人员的培训计划
  - 审计工具的使用（例如：网络扫描工具、穿透测试工具、日志分析工具等）

- 审计委托书
  - 审计师的责任
  - 审计师的权利
  - 审计师的义务
  - 与委托方的交流

•明确审计任务、审计目标、审计范围、独立性、风险评价、被审计单位的其他要求等。
•对于内部审计师而言，还包括关键成功因素、主要绩效衡量指标及其他工作措施。

•审计师有权接触的相关信息，询问相关被审计人员，巡视被审计场所及信息系统相关的设备、软件等；
•审计人员有权了解组织结构包括向董事会和高层经理汇报的途径
•信息系统审计小组成员不同的权限

•确定报告接受者；质量评估；约定的完工期；预算；双方达成的协议。
•对内部审计师还包括：工作成绩和职责标准；向上级汇报的途径；信息系统审计师的经历与经验；个人工作表现评价；独立性评价；对标准遵守情况；计划完成情况；经费开支

•委托方要准确描述信息系统审计目标、对象、领域和信息系统审计时限；
•描述可能面临的问题的解决方案
•提供能进行有效、便捷的交流方式和工具

- 审计方案(Audit Program)
  - 信息系统审计师经常需要从不同的角度评价IT系统及其功能，此时建立审计工作方案(也就是具体的审计策略与计划)是一件十分重要的工作；
  - 通过审计工作方案可以确定具体的审计范围、审计目标、审计程序，以获得充分的、合理的证据，以得出和支持审计结论与审计建议。

审计方案的一般内容

- 获得对审计领域及审计主题的理解并进行记录；
- 进行风险评估并制定通用的审计计划和日程安排；
- 制定详细的审计步骤；
- 对审计领域及审计主题的预审计；
- 对审计领域及审计主题进行评价；
- 符合性测试(常指对控制的测试)
- 实质性测试；
- 报告(沟通审计结果)；
- 后续工作。

– 编制审计方案要考虑的问题

- 信息系统的使用程度
- 信息系统的复杂程度
- 信息系统的组织结构
- 数据的可获得性
- 计算机辅助审计技术
- 特殊技能的要求
- 收集信息系统环境资料

n 了解被审计单位及其环境

- 企业的组织结构与业务流程
- 权力与责任的沟通手段
- 管理层的监管手段
- 了解业务信息系统
- 了解对审计范围有显著影响的事件

n 审计资源安排计划

- 审计日期安排
- 审计人力资源的确定与培训
- 项目管理
- 可用资源与需求的匹配

n 审计目标

通用审计目标

- 为管理当局提供相关控制已有效实施的保证
- 发现控制弱点和由此而产生的风险
- 为管理当局提出纠正建议

—ISACA　CoBIT框架－审计指南

例如：信息安全审计的目标

- ü为达到控制信息安全的目标，要对委托方提供合理的保证
- ü证明组织存在信息安全控制弱点，并指出这种弱点所产生的风险
- ü建议对信息安全存在的弱点采取控制措施
- ü使委托方管理人员了解组织当前组织信息安全的状况
- ü促使管理者提高信息安全意识

– 确定审计内容重点内容(重要性水平)

- 业务流程分析
- 建立信息系统的轮廓
- 现有控制的初步评估
- 已往审计报告的分析
- 审计师的职业经验

例如：

A组织的须审计的重点内容

- ü总体安全评审
- ü主机与网络安全
- ü物理安全
- ü环境安全
- ü业务应用系统安全
- ü知识产权保护
- ü业务连续性计划

- 日程安排（示例）
  - t-开始审计时间，　　n-周
    - 签订审计委托书　　t-10
    - 确定审计日期　　t-8
      - 到达目的地时间
      - 审计小组工作时间
      - 开始调查时间
      - 结果调查时间
    - 确定访谈对象　　t-8
    - 确定审计小组成员　　t-8
    - 收集文档资料　　t-4
    - 起草审计报告　　t+2
    - 完成审计报告　　t+6

n 资源

n＝周 x 人数

n前期准备	1	
n实施审计	1	(+1 每增加一个主题)*
n完成报告	1	(+1 每增加一个主题)*
n总计	3	(+2 每增加一个主题)

*人员要求见下一页

- 人员要求（示例）
  - 所需人员

    (假设人员都具有足够经验)

    - 总体安全评审 +1
    - 主机与网络安全 +1
    - 物理安全、环境安全 +1
    - 业务应用系统安全 +1
    - 业务连续性计划 +1
  - ----------
    - 最多人数 +5

n 所需经验

- n小组组长 ＞5年
  - n 审计管理 高
  - n 沟通能力 高
  - n 信息系统安全 非常高
  - n 掌握CSA方法 较深
- n主机网络安全 ＞3年
- n物理环境安全 ＞3年
- n业务应用系统 ＞5年
- n业务连续性计划 ＞5年

*所有人员都应有类似的审计经验，否则审计日期的安排至少应该增加50%

理想的小组规模：3－4人

n 信息收集（示例）

n IT系统信息

- 信息安全方针
- 已有的信息安全与IT的调查报告
- 组织流程图
- 联系人姓名与地址
- 网络拓扑与描述
- IT资产分类目录
- 业务连续性计划

n 相关法律与法规

- 组织数据保护/个人隐私
- 计算机犯罪/滥用
- 软件版权
- 知识产权

n IT政策与程序

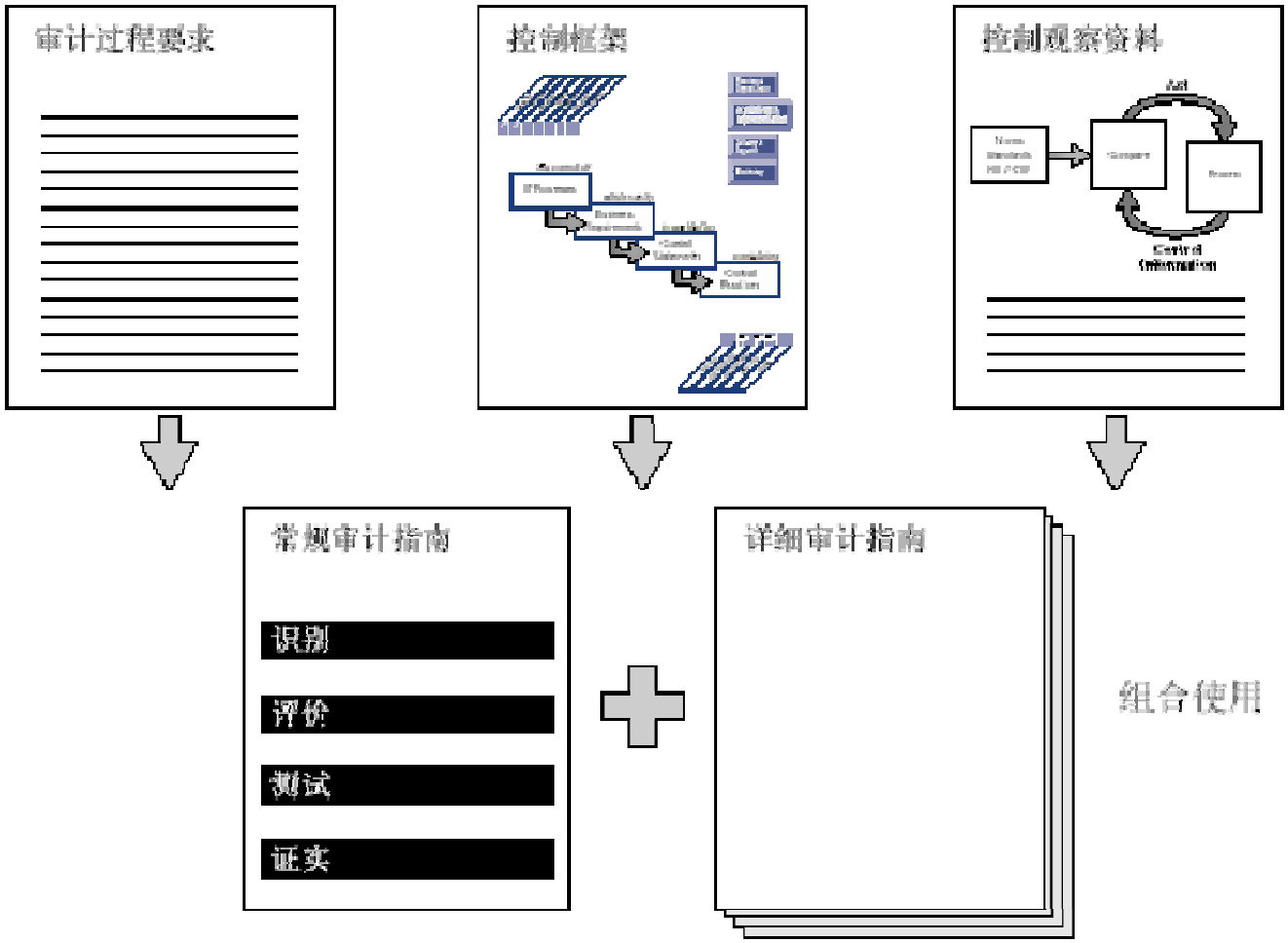
- 信息安全政策
- 物理访问、逻辑访问控制
- 运营管理（备份、日志等）
- 系统开发
- 第三方提供的保险
- 工作描述

n 场地信息

- 建筑平面图
- 机房设计与设备放置
- 防灾措施

3.3 信息系统审计过程

- COBIT推荐的审计过程



– 审计的四个过程

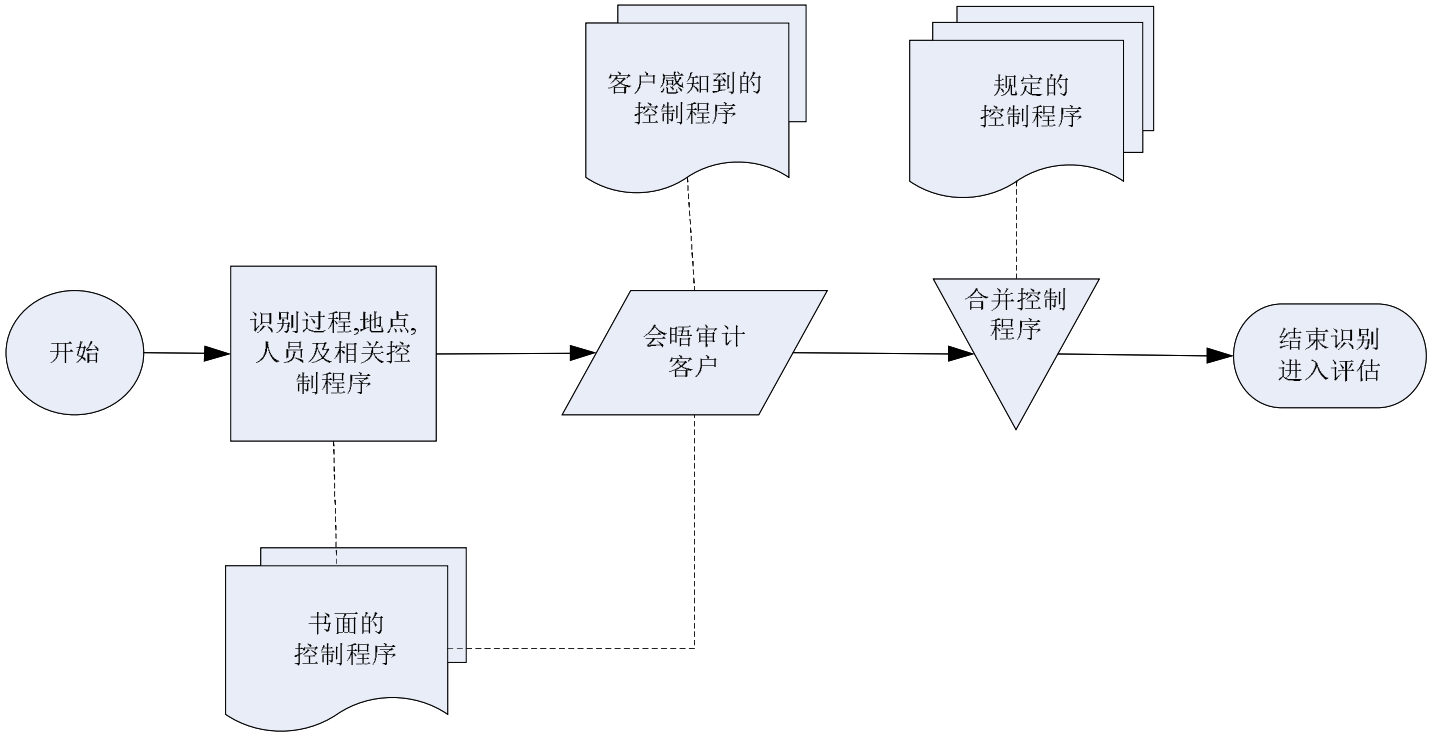
--获得对业务需求有关的风险、和相应的控制方法的理解；

----评价规定的控制的适宜性；

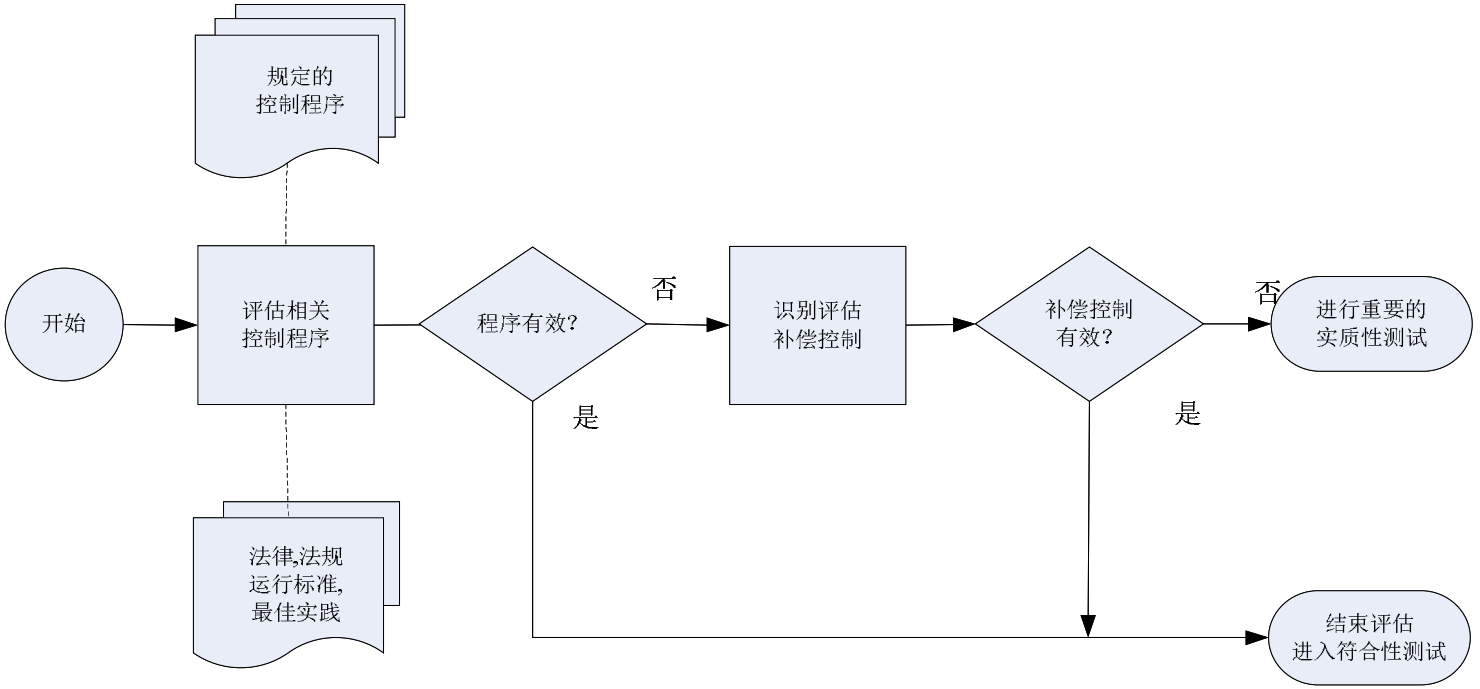
------评估符合性，通过测试规定的控制是否按规定、一致的、持续的起作用；

--------证实，通过分析技术和/或咨询可选的来源，证实控制目标的风险不存在。

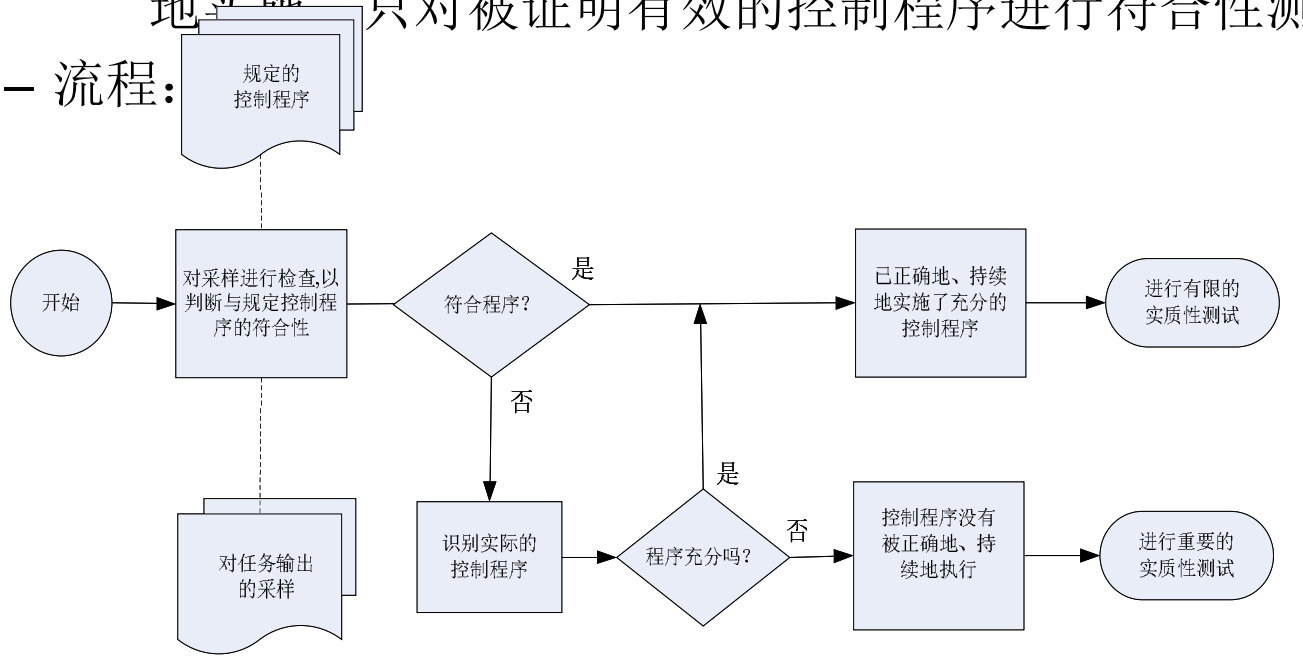
- 审计步骤一：确定与记录
  - 目标：
    - 为了使审计师能够熟悉审计目标所涉及的任务，并且了解信息系统管理层人员是如何确认他们已实施了有效的控制，包括识别出与实施的任务和规定的控制程序相关的人员、过程和地点。
  - 流程：



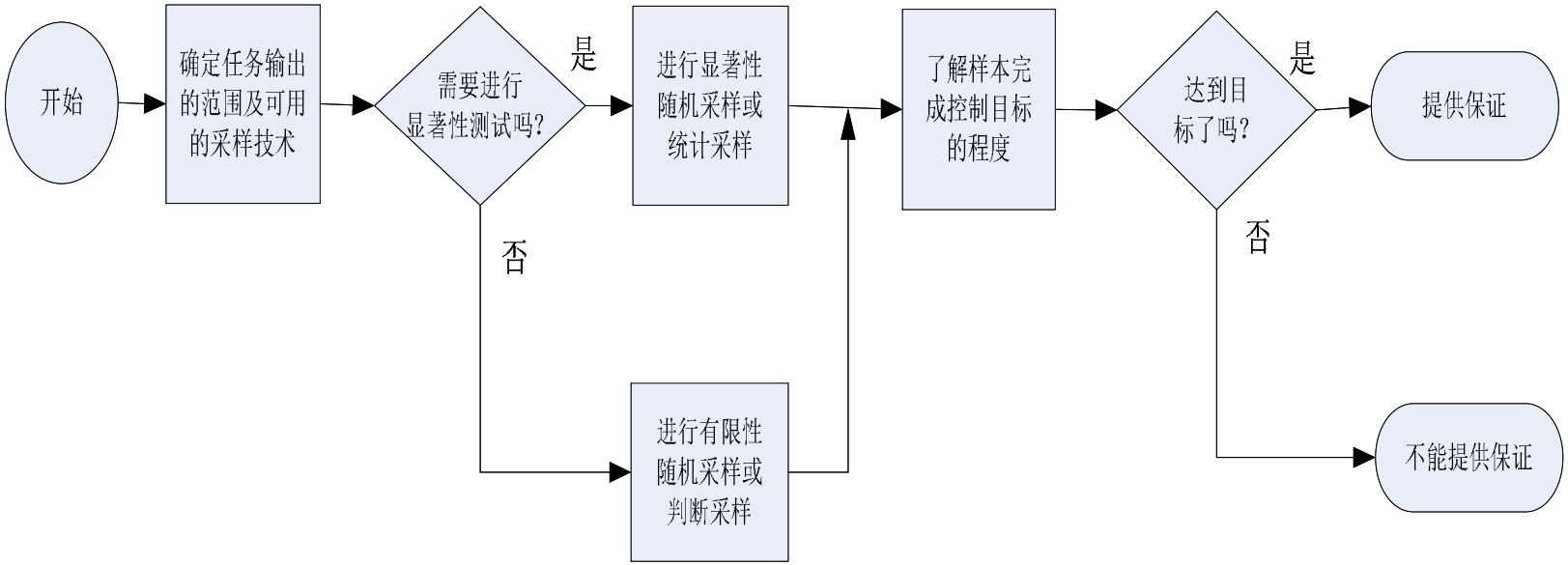
- 审计步骤二：评估
  - 目标：
    - » 通过评估规定的控制程序，以决定此程序是否提供了有效的控制结构。评估时要利用已确定的准则、行业标准及必要的审计判断。
    - » 一个有效的控制结构应当考虑成本有效性，要对任务已被执行、控制目标已达到提供合理保证。
  - 流程：



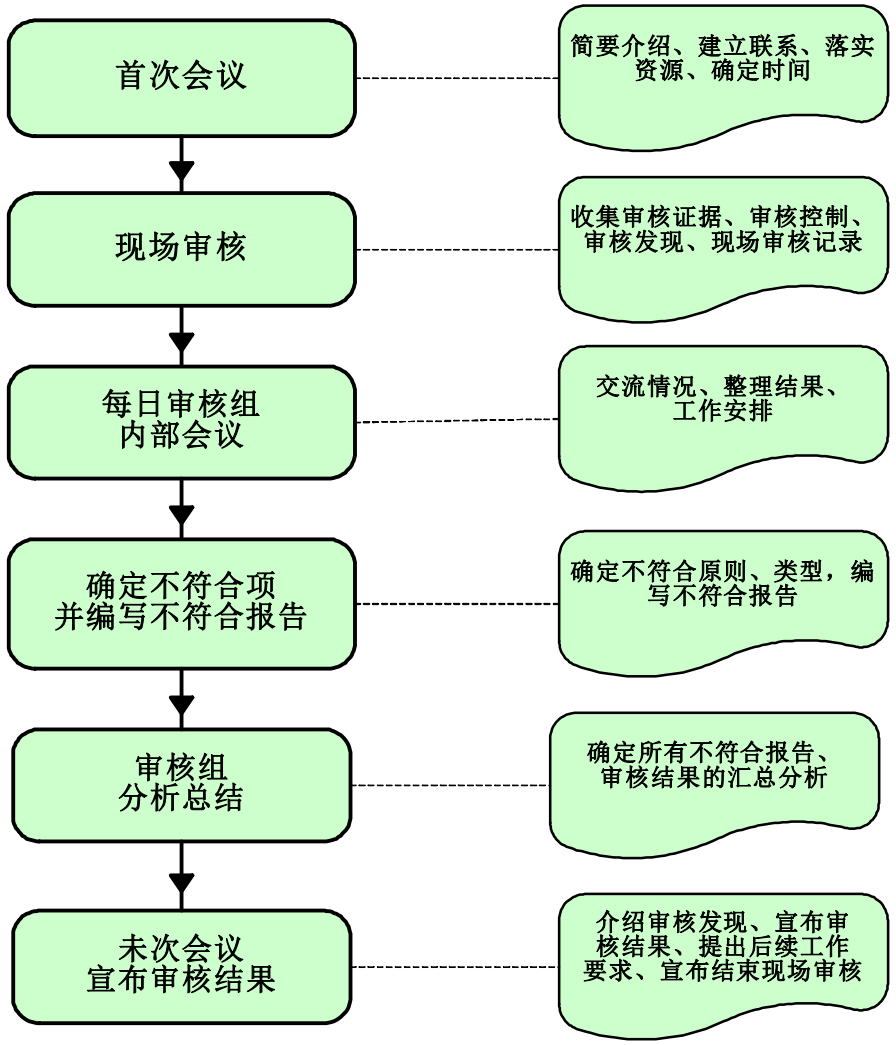
- 审计步骤三：符合性测试
  - 目标：
    - » 对组织符合规定的控制程序的程度进行分析，把实际的控制程序及补偿性控制措施与规定的控制程序进行对比，并进行文档检查、会晤相关人员，以判断控制是否被正确地、持续地实施。只对被证明有效的控制程序进行符合性测试。
  - 流程：



- 审计步骤四：实质性测试
  - 目标：
    - » 进行必要的数据测试，就给定的业务目标是否已达到，为管理层提供最终的保证。
  - 流程：



- 现场审计步骤
  - 预审计计划
  - 首次会议
  - 资料收集
  - 实地检查重要设备与流程
  - 符合性测试、实质性测试
  - CSA工作组评审，得出结论
  - 与被审计方进行沟通
  - 拟定审计报告



- 现场时间安排（示例）

<table>
<tr><th></th><th>星期一</th><th>星期二</th><th>星期三</th><th>星期四</th><th>星期五</th></tr>
<tr><td>08:30－09:00</td><td></td><td rowspan="3">主机及网络安全（网络数据中心符合性测试）</td><td rowspan="4">主机及网络安全（各业务部门符合性测试）</td><td rowspan="3">主机及网络安全（实质性测试）</td><td>对不确定性问题再次确认</td></tr>
<tr><td>09:00－09:30</td><td>开始调查</td><td rowspan="3">与被审计方交流审计结论，取得一致意见。</td></tr>
<tr><td>09:30－10:00
10:00－10:30
10:30－11:00
11:00－11:30</td><td rowspan="2">现场走访，了解概况</td></tr>
<tr><td>11:30－12:00</td><td>提问</td><td>提问</td><td>提问</td></tr>
<tr><td>12:00－13:00</td><td>午餐</td><td>午餐</td><td>午餐</td><td>午餐</td><td>午餐</td></tr>
<tr><td>13:00－13:30
13:30－14:00
14:00－14:30
14:30－15:00
15:00－15:30
15:30－16:00</td><td rowspan="2">主机及网络安全（总体概况，相关安全政策，管理与维护措施）</td><td rowspan="3">评审文档（主机及网络安全程序）</td><td rowspan="4">主机及网络安全（各业务部门符合性测试</td><td rowspan="3">主机及网络安全（穿透性测试）</td><td rowspan="2">进一步整理审计底稿、审计结果汇总，得出此主课审计结论</td></tr>
<tr><td>16:00－16:30</td><td>文档评审</td><td rowspan="3">主机及网络安全主题审计结束</td></tr>
<tr><td>16:30－17:00</td><td>提问</td><td>提问</td><td>提问</td></tr>
<tr><td>17:00－17:30
17:30－18:00
18:00－18:30</td><td rowspan="2">审计小组整理文档，总结交流，第二天安排</td><td rowspan="2">审计小组整理文档，总结交流，第二天安排</td><td rowspan="2">审计小组总结，第二天安排</td><td rowspan="2">审计小组总结，评审底稿，初步审计结果汇总</td></tr>
</table>

- 审计证据的收集
  - 证据就是审计师按照审计标准及目标的要求，在对某一实体或数据进行审计时所采用的信息。
  - 收集证据是审计过程的一个重要步骤，信息系统审计师必须了解审计证据的表现形式、收集及评价证据的程序与技术
  - 证据的可靠性保证：

u 提供审计证据人员的独立性

u 提供审计信息或证据人员的资格

u 审计证据的客观性

u 审计证据的时效性

- 收集证据的方法
  - 观察
    - 在被审计方办公场所内外进行观察
    - 从地下室到建筑物屋顶
    - 观察员工形为
    - 观察对来访者的接待
    - …
  - 检查文档
    - 对所有收到的文档进行标记(时间、日程、来源、格式)
    - 生成并维护一个文档列表
    - 对控制进行突出显示
    - 列出所缺文档（或不清楚的内容）
    - 一些样例文档的拷贝（供受审计方参考）
    - …

- 人员访谈
  - 各种人员交流、讨论，发现问题
  - 测试安全意识与技能
- 音像资料获取
  - 对一些需要记录的重要场所与人员行为，用录音、录像方式记录
- 信息系统审计证据的获取
  - 辅助审计软件
  - 网络扫描工具
  - 穿透测试工具
  - 口令测试工具

- 审计证据评价
  - 收集审计证据之后，要评估所收集的信息，以便提出审计意见。
  - 审计证据评价要考虑的因素有：
    - 控制需求
    - 相关及周边信息
    - 考虑补偿性与重叠性控制
    - 考虑控制的相关性
    - 判断控制是否有效率和效果
    - 分析证据的技术
  - 判断审计结果的重要性水平
    - 审计师应善用判断来决定哪些问题对相关层级主管是重要的，并向他们报告。

- 审计报告
  - 审计准则070.03中规定“在信息系统审计完成后，信息系统审计师应提交一份按要求格式书写的信息系统审计报告。
  - 信息系统审计报告应陈述信息系统审计工作的范围、目标、期间、性质等，并限定报告提交对象和发放条件。在报告中还应陈述信息系统审计结论、信息系统审计建议和保留意见。”
  - 审计指南070.010“审计报告”提供了一个审计报告内容与格式的一般指导

- 信息安全审计报告示例

- 介绍
  - 委托书（审计目标和范围）
  - 审计过程（日程，活动）
- 审计总结
  - 审计重要发现综述
  - 审计结论
  - 主要建议
  - 管理层对审计结论的反应
- 总体安全评审
  - CSA方法介绍
  - 安全评审的结果
  - 详细发现与建议
- 主机与网络安全
  - 评审的结果
  - 详细发现与建议
- 物理安全、环境安全
  - 评审的结果
  - 详细发现与建议
- 业务应用系统安全
  - 评审的结果
  - 详细发现与建议
- 业务连续性计划
  - 评审的结果
  - 详细发现与建议
- ……..
- 附录
  - CSA分值列表

3.4 审计后事宜

- 质量保证活动
  - 审计小组
    - 遵守审计程序与步骤
    - 使用检查列表
      - 使用与审计内容相关的检查列表
      - 根据列表提出问题
      - 审计发现与建议
    - 审计质量控制标准
    - 计算机辅助审计
    - 每天审计小组讨论与检查
    - 与委托方讨论审计发现
    - 主任审计师对审计结论的复核

- 委托方
  - 对以下活动要进行核实和签署意见
    - CSA评审意见
    - CSA评分的更改
  - 审计报告
    - 阅读并校对
    - 写委托方的总结
    - 对审计建议进行核对

三人行，必有我师

- 审计跟踪
  - 审计工作应当是一个持续进行的过程，某一阶段审计活动完成，审计报告递交后，还需要跟踪检查管理层是否就审计发现及结论采取了改进措施。
  - 跟踪检查的时效性取决于审计发现的重要性及基于审计的职业判断，跟踪检查的结果要及时与管理层沟通。
- 审计文档（审计底稿）
  - ISACA审计指南060.010“审计文档”条款对审计文档作了明确的要求.
  - 应当包括：审计计划、信息系统环境的描述及图示、审计程序、会议记录、审计证据、审计发现、审计结论及建议、审计过程中发布的任何其他报告及监督检查结论等。

谢谢

三人行，必有我师

ITIL先锋论坛，汇聚IT服务管理大师们的力量