赛迪顾问信息化管理丛书

HZ BOOKS
华章经管

# 信息系统审计

## 安全、风险管理与控制

孙强　主编

机械工业出版社
China Machine Press

赛迪顾问信息化管理丛书

# 信息系统审计

## 安全、风险管理与控制

孙强 主编

本书是为四类读者写的：一类是管理人士，本书阐述了信息化的整体概念，描述了管理层与咨询和技术服务提供商沟通的共同语言，以及将IT管理与公司上层活动整合起来的方法。第二类是IT的高级管理者和那些准备向管理阶层迈进的IT人士，本书介绍了国际上公认的最权威、最全面的评价和指导IT控制的方法论及其模型。第三类读者是注册会计师及管理咨询顾问，他们在精通管理和专业的同时还急需加强信息系统和网络技术领域的知识。第四类是准备通过国际信息系统审计师或我国信息系统工程监理工程师认证考试的人员，由于信息技术的国际性，本书同样会对这类读者的工作与学习有较大帮助。



**图书在版编目（CIP）数据**

信息系统审计：安全、风险管理与控制/孙强主编．-北京：机械工业出版社，2003.9

（赛迪顾问信息化管理丛书）

ISBN 7-111-12170-8

Ⅰ.信… Ⅱ.孙… Ⅲ.信息系统-应用-信息管理 Ⅳ.F713.36

中国版本图书馆CIP数据核字（2003）第037050号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：李 阳 陶 宏 李文静 版式设计：刘永青

北京瑞德印刷有限公司印刷·新华书店北京发行所发行

2003年9月第1版第1次印刷

787mm×1092mm 1/16·37.75印张

定价：68.80元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

本社购书热线电话：（010）68326294

# ◆编委会◆

# 推荐序

## 中国人民银行支付与科技司司长　陈　静

作为现代经济的核心，银行业多年来都十分重视信息化建设。从“六五”做准备、“七五”打基础、“八五”上规模、到“九五”见成效，从小到大、从单项业务到综合业务、从单一网点到全国联网，我国已经逐步形成了银行信息化的基本框架，取得了显著的社会效益和经济效益。

在加快实现银行信息化的过程中，我们越来越关心两个问题：一是如何保证信息化项目的合理性、有效性及经济性；二是如何确保项目的可用性及安全性。

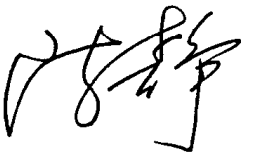
随着信息技术在银行普遍、深入的应用，银行信息系统的正常运行已经成为银行业务正常运营最基本的条件之一。银行信息化涉及政策、管理、技术、产品等各个方面，如何实现信息化的预定目标同时规避信息化过程中各个环节的风险，保护银行的信息资产，是国内外银行界普遍关心的问题。意外灾祸、系统故障、人为操作不当、安全管理及措施的漏洞等都有可能造成信息系统不能正常工作，影响到银行业务的正常运营。信息安全越来越成为银行信息化建设与管理中需要密切关注的问题。如何保证银行核心数据的安全，如何建立完善的应急管理机制等已是目前迫切需要解决的问题。

美国等市场经济发达国家很早就开展了由独立资格的第三方进行的信息系统审计工作，建立了完善的信息系统审计体系。特别是美国“9·11”事件和前一阶段蔓延的SARS疫情，使我们对信息系统的安全性和应急管理等概念有了全新的认识。信息的“保密性、可用性和完整性”的实现仅仅靠技术与产品的组合是远远不够的，应该是在风险分析的基础上，结合管理、技术、产品、法律、环境等综合因素，制定控制目标与控制方式，从而建立一整套严密的安全保障体系。这些都需要通过独立的第三方审计来监督和保证。目前，我国银行业对信息安全的重视程度和需要，已从单一的产品和技术向整体解决方案过渡，同时从封闭式的设计、实施与管理，不断与完善的、具有适当资质的、独立的第三方审计相结合，这是未来的一个发展趋势。

赛迪顾问股份有限公司孙强先生主编的这本书可谓是应时而生，此时把信息系统审计的思想与方法引入国内是很有意义的。本书有两个突出的特点：一是全面和系统地介绍了信息系统审计的基本概念、理论方法、具体实例，从信息系统的规划、系统平台建设、应用开发、运营管理、灾难恢复与业务持续计划的审计，到企业风险管理、电子商务、电子政务、信息系统工程监理等目前热点话题都有较深入的涉

及，可指导信息系统审计人员系统准确地把握信息系统审计思想，正确地运用信息系统审计方法与技术。二是观点的组织与题材的把握上，有许多独到的观点，与国内的实际结合较好，有较好的参考、指导价值。

总之，在信息化过程中，信息系统审计的作用是无可替代的，是我们在加快信息化建设过程中一项十分重要的工作。我们应该结合国情大力宣传、积极推广信息系统审计，加快培养专业的信息系统审计人员。本书在这方面进行了开创性的探索，我相信它可以为国内即将蓬勃展开的信息系统审计工作发挥积极的作用。



# 推荐序

审计署信息化建设领导小组成员
审计署计算机技术中心主任　王智玉

信息系统审计是做什么的？它做审计吗？它与国家审计机关、注册会计师从事的审计有什么关系？都是有争议的事情。信息系统审计的全称应当是信息系统审计与控制（Information System Audit and Control），其协会会员称之为注册信息系统审计师（CISA，Certified Information System Auditor），确实用了“Audit”、“Auditor”两个词，但是它所从事的工作，与目前国人所理解、所熟知的、国家法律规定的审计，在内容上有相当大的差异。

审计署曾给审计下过一个简明定义：“审计是独立检查会计账目，监督财政财务收支真实、合法、效益的行为。”《注册会计师法》关于会计事务所从事审计业务的内容确定为两条：审查企业会计报表、验证企业资本。按照这些说法，审计的工作对象都是与记载财政财务收支及其相关经济活动的载体——账目有关系的。

可是信息系统审计的工作对象就要宽泛得多了。对于信息系统审计中使用的“Audit”一词，国内有关权威单位曾经意译为“审记”。例如：科学技术部、财政部、国家税务总局2000年《中国高新技术新产品目录》应用软件部分中，就列入了“审记软件”，并给予了界定条件描述：“对计算机上的通信和操作的内容进行采集、分析、追踪、审查，提出警告信息，并给予日志性记载。”虽然“审记”这个词汇没有被公众所接受，但它对“审记”概念的描述是准确的，“审记”的对象进一步扩大为整个信息系统时也是适用的。

即使国家审计机关、会计事务所的工作对象仍然局限在查账上，由于会计电算化的普及、ERP的应用，信息系统审计也有了用武之地，因为账不再仅仅是纸质的。信息化条件下，审计人员如果仅仅对计算机、财务软件中保存运行的数据进行计算、核对，而没有能力对处理财政财务业务的信息系统进行检查，很可能形成信息化条件下的“假账真查”。于是审计和“审记”就有了一个交集：当信息系统中处理的是财政财务信息时，“审记”的内容和方法可以服务于审计。

近五年来，审计机关在对计算机管理的财政财务电子数据进行审计的时候，已经发现了利用会计软件、管理软件作弊的案例，由此开展了对计算机信息系统的审计。这种审计属于很初级阶段的，最显著的特征一是仍然围绕财政财务收支审计，二是大多数情况下是由于在电子数据的审核中发现了问题，株连到信息系统，“拔出罗卜想起了泥”，进一步“带出泥”。国家对审计机关探索信息系统审计并取得显著成效给予了充分肯定。2001年国务院办公厅下发的《关于利用计算机信息系统开展

审计工作有关问题的通知》，明确规定审计机关有权检查被审计单位运用计算机管理财政收支、财务收支的信息系统；被审计单位应当按照审计机关的要求，提供与财政收支、财务收支有关的电子数据和必要的计算机技术文档等资料；被审计单位的计算机信息系统应当具备符合国家标准或者行业标准的数据接口；审计机关发现被审计单位的计算机信息系统不符合法律、法规和政府有关主管部门的规定、标准的，可以责令限期改正或者更换；审计机关在审计过程中发现开发、故意使用有舞弊功能的计算机信息系统的，要依法追究有关单位和人员的责任；审计机关对被审计单位电子数据真实性产生疑问时，可以提出对计算机信息系统进行测试的方案，监督被审计单位操作人员按照方案的要求进行测试。

前不久，审计署制定了新的五年规划，其中一个非常重大的变化就是提出五年内逐步做到财务收支审计项目和效益审计项目各占一半。这是中国国家审计工作重点的一个里程碑式的转变。中国审计机关从此也可能开始逐渐关注信息系统整体的安全、风险、管理、控制，不管它与财政财务收支是否有直接的关系。

审计工作不局限于财政财务收支在国外有充足的先例。9·11之前，美国审计署检查了全国30多个机场，对机场的安检设施和制度提出了警告；还乔装打扮，试探美国国防部的保卫工作，结果连过三道门岗如入无人之境，审计报告引起轩然大波。英国审计署对情报部门的笔记本计算机保管使用情况进行审计，查出几十台可能装有国家机密信息的笔记本计算机下落不明。澳大利亚审计署就“为了有效保卫澳大利亚，应当发展空军还是应当发展坦克”发表过审计报告。以色列审计署推行的政策审计，50%以上的项目与账目无关。内部审计师具有冲破财政财务收支范围的内在动力，1999年，国际内部审计师协会给内部审计下了这样的定义：内部审计是旨在获取附加价值，改善组织业务而设计的具有独立性和客观性的保证和咨询活动。它通过提供系统的严格的方法来评价和提高风险管理、控制以及治理程序的有效性，借以协助组织实现其目的。受安然事件和安达信舞弊丑闻的影响，注册会计师从事管理咨询活动势头受挫，人们可以相信利益驱动必然会使注册会计师以种种合法外衣涉猎咨询服务。而信息系统的审计，之所以成为国外国家审计、内部审计、社会审计各方积极研究、探索、参与的新领域，无论从哪个角度讲都是道理充分的。

在审计和“审记”关系处理上，孙强在《信息系统审计》一书中采取了相互融合的办法，使二者得到了较好的统一。首先他对审计的定义把检查的范围确定为“可计量的信息证据”，既跳出了“会计账目”，又轻松地将“会计账目”收入囊中。其次，审计判断标准确定为“与既定标准的符合程度”，同样既包括“真实、合法、效益”，而又不限于此。基于融合的思路，书的前半部分讲了审计，后半部分讲了“审记”。在书的前言中，孙强讲《信息系统审计》的读者群有四类人——管理人士、IT人士、审计人员、有志于成为信息系统审计师的人士。那么《信息系统审计》的前半部分主要是给除审计人员以外的三类人看的，使他们学习用审计的思维看待信息系统。《信息系统审计》的后半部分是重点，也是此“审记”区别于彼审计的核心

所在，所讲所述，读有所值，对于各类读者都应当说是开卷有益。

目前，关于信息系统审计的书不多，尚属于“一阵新风吹过来”的阶段。作为在审计信息化方面负有一定责任的国家审计工作人员，我为这本书的出版感到高兴，毕竟大家都在关注信息系统的审计，这对于信息系统的审计是基础，是希望所在。

王智玉

# 推荐序

国家信息中心副主任　徐漳河

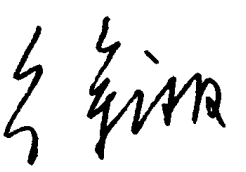
不管人们情愿不情愿，认可不认可，当今世界经济和社会发展的两大趋势是政治多元化和经济一体化。当然，推进和阻滞两大趋势的斗争是激烈的、长期的。伴随而来的重要时代特征之一，则是信息化、网络经济持续迅猛发展日益成为人类社会经济发展的强劲动力，成为判定一个国家和地区现代化程度及综合国力强弱的重要因素之一。

中国在“以信息化带动工业化，以工业化促进信息化，加快建设有中国特色的社会主义现代化”方针指引下，呈现一派勃勃生机，在国际事务中也担负了更多的责任，发挥了越来越大的作用。

回顾我国信息化近十多年来的发展进程，既应肯定信息化工作取得的显著成绩及信息化对社会经济发展的巨大推动作用；也应承认存在的差距和不足，认真地进行反思，探索解决问题的途径和办法。对一些现实的和深层次的问题，例如：对信息化建设成本绩效分析，信息技术如何更好地促进政府职能的转变，如何提升企业的核心竞争力，如何规避风险、拓展业务和市场等都应该进行深入的研究。

信息化管理是我国信息化建设领域中一个十分重要的研究和实践课题，是现代管理理论和手段在信息化建设中发挥主导作用的根本之所在。当前我国信息化建设中存在的突出问题，有来自技术方面的原因，但更重要的是管理观念、思路以及预期方面的原因。有什么样的管理水平，就会产生什么样的运行和经营效果。中国的信息化建设应该借鉴国际上成功的经验和做法，更应该探索走有中国特色的信息化之路。

中国电子信息产业发展研究院下属赛迪顾问股份有限公司组织有关专家持续跟踪国际上IT管理与控制的最新研究进展，并结合我国信息化建设中出现的热点、焦点和难点问题多次进行了专题研讨。在此基础上，将有关研究成果汇编成册，引述和推介了信息化建设项目的决策论证，风险分析，绩效量化，评价指标体系建立等方面的理论和经验。其中，对理论上有争议，尚无定论的问题采取了“百家争鸣、兼容并蓄”的科学态度，供人们研究参考。本书涵盖体系比较完整，内容较为充实，具有较好的参考和实用价值。不仅适合于信息化工程技术人员培训及MBA教学的需要，也适合于信息化管理咨询人员的工作需求。衷心希望本书的出版不违初衷，在我国的信息化建设事业中发挥其应有的作用。



# 推荐序

## 北京甲骨文软件系统有限公司北方区董事总经理　胡伯林

目前，“公司治理”（Corporate Governance）问题因上市公司频频“惊曝黑幕”而成为全球性的话题。无论是在美国出现的安然、世通、施乐等粉饰业绩甚至导致企业崩溃的案件，还是在日本出现的雪印食品公司舞弊案件，亦或是在中国出现的蓝田股份和银广厦的利润神话破灭事件，使公司治理成为企业高层议事日程中最重要和迫切的任务之一。

在中国，由于治理主体的明晰和到位，作为公司管理基础提升的公司治理已经成为现实问题。推进公司治理，建立规范、高效的现代企业制度，使企业运行的每个环节都处于规范和可控制状态，达到“透明、控制和效率”的治理效果，正是中国国有企业改革和上市公司治理所要努力的方向。

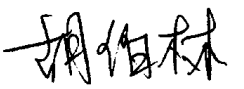
业界普遍认为，以公司治理的法规和原则为标准，以信息技术为平台，以统一、真实、及时的公开信息为结果的公司治理才是良好的公司治理。甲骨文公司提出，良好的公司治理体系必须包含可见性（visibility）、控制力（control）和高效率（efficiency）三个关键因素。可见性是指企业要有一个覆盖整个企业的安全、透明的流程，使得高层决策者能够得到实时的、准确的、中肯的和一致的信息。并且，这些信息应该是可以能够被细查到企业的任何组织层次、任何业务环节。控制力是指企业要建立集中管理的内部流程，利用完整、安全，并且容易获得的企业活动的历史记录来实现对整个企业的控制。效率是指企业能够迅速准确地收集、调整财务数据，把建立集中处理、降低成本、减少风险的流程作为贯穿企业治理的主线，以降低管理费用和降低风险。

甲骨文公司治理解决方案的推出从技术层面上解决了公司治理的难题，这对中国公司治理进程发展来说意义重大。完全自动化的信息处理可以减少发生错误的风险，降低信息处理的成本，而且能够实现决策者对信息的“实时”需求，让他们可以随时观察企业的运行状态。它同时也为企业提供了及时进行培训和教育的成本低廉、易于考评的信息化手段。

由于甲骨文独一无二地拥有从基础层到应用层的丰富的全线产品和应用方案的实施能力，与那些只专注于某一领域产品的方案供应商相比，甲骨文能够预测从软件成本到实施成本和维护成本方面的所有成本，并且为客户提高真正一体化的解决方案。基于单一数据库核心技术优势的 Oracle 电子商务套件所提供的解决方案既可以大大降低公司治理流程中发生错误的风险，同时也在很大程度上降低了公司治理

的总体拥有成本（TCO）。同时，由于甲骨文的产品支持 Linux 系统，可以保证甲骨文公司的治理解决方案运行得更快，更经济。

中国电子信息产业发展研究院（CCID）及下属赛迪顾问股份有限公司为推动中国的信息化进程起到了很大的作用，这次编辑出版《赛迪顾问信息化管理丛书》，具有较强的可操作性和指导性。我发现，良好的公司治理的原则和观点在《信息系统审计：安全、风险管理与控制》里有着具体的体现，我希望更多的人阅读此书，并为所在企业的 IT 战略规划和公司治理战略规划提供帮助。



# 推荐序

## 德勤华永会计师事务所有限公司合伙人　Peter Koo

近年来，中国经济不断迅速增长，加入WTO，外国的投资大量涌入，使公司治理逐渐为大多数人所关注。尤其对于大型的企业，公司治理更是至关重要的任务。随着社会、企业信息化的发展，信息技术成为重要的管理工具，IT治理也已经成为法人治理不可分割的组成部分。今天，中国正经历着一场历史性变革，即“以信息化带动工业化，以工业化促进信息化”。信息系统审计应运而生，它不仅是促进法人治理和信息化的重要途径，也是传统审计迈向信息化的关键一步。

作为经济鉴证类社会中介组织，注册会计师行业在提高市场经济运行的有序性、促进专业技术服务的社会化以及提高企业宏观和微观管理水平等方面均发挥着不可替代的作用。在新的时代中，注册会计师行业如何拓展新业务并保持像诸如财务报表鉴证一样稳固的市场地位？回答是：开展和加强信息系统审计业务。然而，大多数传统审计人员并不一定具备有关的内控知识和技能，甚至不知道信息系统审计为何。

所谓信息系统审计是指，审计人员接受委托或授权，收集并评估证据以判断计算机系统（信息系统）是否有效做到保护资产、维护数据完整并最有效率地完成组织目标的活动过程。它既包括信息系统外部审计的鉴证目标——即对被审计单位的信息系统保护资产安全及数据完整的鉴证，又包含内部审计的管理目标——即不仅包括被审计信息系统保护资产安全及数据完整，而且包括信息系统的有效性目标。

《信息系统审计：安全、风险管理与控制》这本书不仅涵盖了注册会计师应该基本了解的关于如何开展信息系统审计工作和相关非传统审计的知识，如注册会计师应该了解的专业词汇、判断方法、信息系统审计程序以及审计报告等，还包括具体实施过程中应采取的措施及案例，是一本目前市场上少有的、比较全面的专业书。我很乐意向IT人士、注册会计师、IT咨询顾问以及企业管理人员推荐此书，希望这本书能够有助于他们了解认识信息系统审计，并积极参与其中。

AHKSA，CA，AICPA，CFE，CISA，CRP，Lead BS7799 Auditor
合伙人
企业风险管理服务
德勤华永会计师事务所有限公司

# 前　言

## 写作背景

全球化竞争时代已经到来。各组织忙着重组，同时发挥不断增长的IT优势以提高它们的竞争能力。业务重组、裁员、外包、充分授权、扁平化组织和分布式处理都影响着商业和政府组织运作方式的变革，这些变革正在或即将对全球范围内组织的管理和运作控制结构产生深远的影响。

在加速变化的框架内，强调获得竞争优势和降低成本意味着对信息技术更多的依赖。可是如何建立和运营与业务战略目标“精确校准”的信息系统，这就要求管理者和信息技术专家必须进行合理的分析和谨慎的判断，必须理解有关控制技术及其变化着的特征。鉴于信息技术的飞速发展，他们的技能必须与信息技术和环境保持同样快速的改进。这对于管理者和信息技术专家而言，是一个很大的挑战。

目前从国际来看，既懂业务又懂信息技术的信息系统审计师在这方面走在时代的前沿，他们通过对内部或第三方提供的IT服务进行鉴证和审计，来确保IT和业务的融合以及充分的安全和控制。另外，信息系统审计师也越来越多地被管理者请去，就IT管理、信息安全和控制相关的问题提供预防性的咨询和建议。

事实上，信息系统审计在我国也开始起步并迅速发展，国家在此方面的法律法规已经或正在出台，跨国公司和金融业等开始定义信息系统审计职位，国际会计公司在此领域正在加大投入，可以预见信息系统审计在我国即将迎来大发展的黄金时代。

## 面向读者群

《信息系统审计：安全、风险管理与控制》是为四类读者而写的：一类是管理人士。管理人士通过此书可以了解信息化的整体概念，掌握与管理高层（董事会）、咨询和技术服务提供商沟通的共同语言，以及将IT管理与公司上层活动整合起来的方

法。对第二类读者，即IT的高级管理者和那些准备向管理阶层迈进的IT人士，本书介绍了国际上公认的最权威、最全面的评价和指导IT控制的方法论及其模型。对于如何组织和理解大量IT运作上的细节性问题，本书提供了方方面面的最佳实务指导。准备向管理阶层迈进的IT人士通过此书，学习“像管理者一样思考”。当然，本书也为他们提供了一种共同的观点和相互交流的语言。第三类读者是注册会计师或管理咨询顾问，面对新经济时代的机遇与挑战，他们在精通管理和专业的同时还急需加强信息系统和网络技术领域的知识。第四类读者是准备通过国际信息系统审计师或我国信息系统工程监理工程师认证考试的人员，由于信息技术的国际性，本书同样会对他们的工作与学习有较大帮助。面向以上四类读者的专著在国内极为匮乏，我们希望通过此书抛砖引玉，向同行学习，共同切磋，以求信息系统审计能有更大的发展，真正地为我国的信息化建设保驾护航。

## 本书主要内容与使用方法

本书的最大特色体现在结合中国国情，引进、消化和吸收了国际上先进的安全、风险管理与控制的方法论和最佳实务。

全书分为四篇：

第一篇简要概述了审计的基本知识，这包括审计的概念，内部控制及其测试与评价，审计报告，职业道德等。审计专业的人员可以跳过此部分，但建议从事IT工作的人员及参加国际信息系统审计师认证考试的人员详细阅读。

第二篇为信息系统审计理论，简要概述了信息系统审计的起源与发展，信息系统审计计划、信息系统环境下的内部控制及其测试与评价、审计证据的收集与评价以及信息系统审计报告等。

第三篇为信息系统审计实务，基本上依照信息系统建设和运营维护生命周期的逻辑关系，详细描述了信息系统的战略规划与组织，技术基础平台建设，应用系统的建设，信息系统的建设和运营实务，灾难恢复和业务持续计划等，同时还介绍了具有中国特色的信息系统安全、风险与控制制度——信息系统工程监理的相关内容。关于此部分内容，IT专业人士可以跳过技术概念部分，重点阅读对各项技术的审计部分。

第四篇为信息安全审计实务，信息安全审计是信息系统审计的一个组成部分，鉴于信息安全的重要性，本书将之独立成篇。本篇涵盖信息安全的法规和标准、信息安全审计、信息安全治理、我国电子政务信息安全标准体系等方面内容。

## 本书的撰写

全书由孙强、孟秀转进行整体架构与思路的设计，初稿第1章～第5章、第6

章第1节、第3节、第9章第4节的部分内容由尹夏楠编著，绪论、第6章第3节、第7章～第13章、第21章第1节由孟秀转编著，第14章～第23章由孙强、郝晓玲、王东红、赵刚、李长征编著，第24章～第28章由孙强、王东红、郝晓玲、李长征、邱世明、左天祖、程华等编著。俞静参与了第1章、第2章、第3章的部分修改。全书由孙强、孟秀转总纂定稿。

由于信息技术突飞猛进，信息系统审计涉及的知识范围非常广泛，书中有一些没有进行深入讨论和清晰阐述的问题，读者朋友可以通过访问中国IT治理论坛(www.itg.org.cn)，查看最新的资料，其中包括国内外众多知名公司或协会组织专为本书提供的丰富的软件和案例等，我们也希望能够通过这一互动网络平台，与更多的读者朋友一起交流探讨。对本书内容有任何建议或意见，请填写本书所附的读者调查表（可从www.itg.org.cn上下载）或发电子邮件至：sun6869@sohu.com，您将成为中国IT治理论坛的高级个人会员，并有机会获赠全套丛书。

**赛迪顾问股份有限公司**

# 绪　论

## 审计与信息系统审计的定义

### 审计的定义

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。其目的在于确定、解除被审计单位的受托责任和加强对被审计单位的管理与控制。

理解审计定义，要从以下几点把握：

(1) 审计的主体是“有胜任能力的独立机构或人员”。独立的机构是指政府审计机关、内部审计机构和会计师事务所，独立的人员是指专门从事政府审计、内部审计工作的人员和依法经批准执业的注册会计师。由于审计的专业性要求，对从事审计的机构与个人都要求具有完成审计工作所必须的专业知识与技能，必须熟知既定的标准，并且能够确定为得出适当结论所需审计证据的类型和数量。同时审计机构与人员必须不仅在形式上而且在实质上保持独立的态度。否则，不能从事审计工作。

(2) 审计的关系是由“接受委托或授权”形成的。一般来说，注册会计师审计业务都是接受委托来进行的，而政府审计和内部审计则多是由上级主管部门或领导授权的。

(3) 审计对象是“可计量的信息”。可计量的信息可以有很多形式，但共同的特点是有可确认、证实的形式。比如财务报表、完成工作所需时间、建设支出费用等。

(4) 审计工作的执行和对审计对象的判断是依据“既定标准”。既定标准是指判断认定时所使用的标准。这些标准既可能是立法机关所制定的法律法规，或管理当局所制定的预算或其他绩效衡量标准，也可能是权威团体所颁布的一般公认的准则。