it 审计工作总结（共 6 篇汇总）

第 1 篇 IT 审计知识总结

IT 审计知识总结

IT 审计的出处源自 60 年代 IBM 出版的《Audit encounters Electronic Data Proceing 》等有关在 EDI 环境下进行审核和组织的论述。不久后有关该方面的研究结果不断涌现， IT 审计的雏形初步形成。但是由于信息系统在社会上尚未得到较为广泛的应用，因此 IT 审计并未在社会上形成意识。

七十年代中后期到八十年代初由于计算机在发达国家的企业初步普及，利用计算机犯罪和计算机系统失效的事件频频出现，使得 IT 审计日益得到社会重视，美国、日本先后成立了 IT 审计方面的协会组织。从事对 IT 审计规则的制定和实施指导。值得注意的是 1985 年日本政府出台了《IT 审计标准》并根据美国劳工部的《Skill Start 》和 Northwest Center for Emerging Technologies （NCET）对 IT 信息人员的从业技能的要求制订了 IT 审计师（系统监查员）的技能标准并以之作为新的 审计师（系统监查员） 级考试的参考标准。

九十年代是 IT 审计的普及期，这主要归功于互联网的普及。互联网的普及是利用计算机犯罪的人员温床，此外日益严重的软件项目失败问题引发了是否要对信息系统的投资和开发进行审计的深思。IT 审计得到了前所未有的重视。IT 审计知识概括如下

一、什么是 IT 审计

IT 审计就是信息系统审计，也称 IT 监查，是独立于信息系统本身、信息系统相关开发、使用人员的第三方。IT 审计师采用客观的标准对信息系统的策划、开发、使用维护等相关活动和产物进行完整地、有效地检查和评估。

二、IT 审计的对象和范围

IT 审计涉及整个信息系统的生命周期，IT 审计不是单纯强调对软硬件的审计。它的审计对象涵盖整个信息系统所有活动和中间产物，并包括信息系统实施相关的外部环境。一般来说，对企业实施 IT 审计

的对象有本企业内的IT审计师、外部IT审计事务所委托审计师和国家审计机构。IT 审计按照信息系统的生命周期分为业务计划审计，业务开发审计、业务执行审计和业务维护审计以及涵盖整个信息系统周期的共通业务审计。

1）业务计划审计主要面向信息系统的企划，对信息系统的投资可行性，系统规划与公司战略的相关性，系统开发计划的可行性以及系统需求的完整性和正确性进行审核和验证。 2）业务开发审计对信息系统开发的各个阶段的相关人员的活动、信息、中间产物进行审核，确认这些活动、信息和中间产物的规范性、有效性和对于信息系统目标的针对性。

3）业务执行审计确认与信息系统运行相关的数据、软硬件、安装环境等是否符合信息系统的运营要求，同时对信息系统的功能、性能、易用度、可操作性等进行评估。

4）业务维护审计对信息系统的维护活动和维护结果实施审核和评价。发现在维护中可能出现的各种漏洞和信息系统维护中急待改善的问题。

5）共通业务审计涉及文档管理、进度管理、人员管理、采购管理、风险管理等，检查这些过程的规范性和有效性，并提出改良建议。

三、IT 审计计划

IT 审计的实施需要制定相应的计划，明确 IT 审计的任务、采用的方法和预期应当达到的效果。该计划在提交经营层确认后得以实施。

IT 审计的审计计划分为两种类型基本计划和详细计划（又称分期计划）。

1）基本计划是一个审计年度内相关IT审计活动的计划，确认年度内 IT 审计的各项任务及其大致时间安排。基本计划需要提交经营层批准。它是对整个 IT 审计年度的活动指引方针。内容包括审计对象、审计场所、审计原则、日程安排等。

2）详细计划（分期计划）针对具体项目（系统）或任务，得到 IT 审计部门领导的许可即可，详细计划需要告知被审计对象。详细计划的内容包括审计对象、目的、审计流程、审计要点、审计时间、相关

人员、审计报告提交事项等内容。

四、IT 审计的任务

IT 审计的任务在于站在客观公正的角度上，收集审计信息，生成审计报告，通过审计报告促成信息系统生命周期活动和成果物的改善。

五、IT 审计制度的建立需要注意三点

作为企业，建立一个完善的 IT 审计制度需要做到以下几点

1）IT 审计师是跨信息技术和审计技术的复合型人才，要实施企业的 IT 审计制度，必须重视和培养合格的 IT 审计师；

2）企业应该建立相应的IT审计部门或审计岗位，确定其部门和岗位职责，并将之置于企业经营者的直接管理之内；

3）企业应该制定相应的 IT 审计准则、实施报表、报告等进行 IT 审计所必须的凭据；

企业在建立 IT 审计制度时应当遵循国家相关 IT 审计的法规并结合本企业的业务实际进行。企业的 IT 审计制度不是一成不变的，根据具体企业的营运情况可以在每个审计年度终结后新的审计年度开始前做相应的修改和增删。

六、IT 审计的意义

实施 IT 审计能够强化 IT 投资效果，提高信息系统的安全性，能够客观评价信息系统及信息系统开发，从社会经济和企业、国家信息化投资、安全等方面都具有极大的意义。

七、从 IT 审计看审计学科的发展

1、IT 审计是技术审计的一个典型，IT 审计师标志着一个新的审计时代——“技术审计时代”的到来

随着经济管理与科学技术的不断结合与日益渗透，现代审计已经远远超出了仅对财务会计进行审查的狭窄范围，不断向管理领域和技术领域渗透。IT 审计是技术审计的一个典型。IT 审计实质上是对计算机软件和硬件及整个信息系统的审计，否则，就不能称为 IT 审计。由于计算机的广泛普及，审计环境发生了巨大变化。假如审计人员只懂传统审计，不懂对计算机软硬件的审计，必然面临可怕的潜在审计风险。在无纸办公条件下，会计及其他信息资料被存入计算机信息系统，

审计人员如不考虑被审单位计算机软件和硬件的安全程度，对被审单位的系统与设备盲目信任，即使懂得计算机的简单应用，也极有可能误入计算机陷讲，后果相当危险。只有对计算机审计风险进行正确估计，根据实际情况决定是否采取相应的信息系统审计对策，并能够在风险较大的情况下针对计算机信息系统（包括硬件与软件）实施必要的技术性审计，才能最终保证审计结果的正确性，防止和降低信息技术条件下的审计风险。IT 审计的重要程度由此可以想见。显然，网络时代的到来已对审计人员提出了掌握过硬信息技术的要求。IT 审计师不仅从事对财务会计、经济管理活动的审计，更重要更关键的是对被审单位信息系统进行技术审计。IT 审计师的产生是审计领域进一步扩大化的重要标志，代表着新的审计时代——技术审计时代的到来。

实际上 IT 审计并不是最早的技术审计。早在 IT 审计之前，就已经出现了各种各样的技术性审计，只不过这些技术审计的技术性不如 IT 审计那样与科学技术紧密相关。例如，质量管理中的技术性审计——质量审计（包括产品质量审计、工序质量审计与体系质量审计等），要求对产品质量进行抽查试验；清洁生产中的技术性审计——清洁生产审计，要求揭示生产技术的缺陷并提出预防和消减污染的机会与对策；能源管理中的技术性审计——能源审计，要求进行能源监测，提出能源技术改造方案；环境管理中的技术性审计——环境审计，要求实施环境质量监测，提出环境改进建议与降低污染方案；如此等等，都是具有不同技术程度的审计类型，从它们的技术性特点归类，可以与 IT 审计并称“技术审计”。

技术审计的产生是科学技术日益渗透、审计范围进一步向技术领域拓展的必然结果。随着科学技术如日新月异和现代审计的不断发展，审计的技术领域将不断延伸，未来的技术审计形式将更加丰富多彩。

2、从 IT 审计看现代审计学科的发展

王光远教授在其名著《管理审计理论》中将审计学科划分为“财务审计”与“管理审计”两大分支，倡导发展管理审计，并认为管理审计以财务审计为基础，前者是后者的发展与延伸。

技术审计是当代科技发展与审计发展相互融合的产物。当代社会

是科学技术飞跃发展的社会，科技的迅猛发展已经给整个社会的经济管理活动造成了巨大影响。正是在科技迅速发展的大背景下才产生了形形色色的技术性审计。技术性审计是在原来的财务审计和管理审计基础上，由于科学技术向经济管理领域的渗透而产生的。然而，到目前为止，技术审计在本

质上并不是独立于财务审计和管理审计的第三大审计分支，而是融于财务审计、管理审计之中的一类审计形态。即在财务审计与管理审计两大分支当中都包含某些技术审计。比如，进行计算机财务审计，主要的或本质上是实施财务审计，但由于计算机软件和硬件对财务信息的巨大影响，也往往不得不对使用的硬件和软件进行审计，这又是技术审计；清洁生产审计实质上属于环境（管理）审计中针对生产过程所实施的技术审计，但这种技术审计又是为进行管理审计服务的，依附于管理审计。

从受托责任理论分析，可以提出“受托技术责任”的概念。在财务审计分支中的技术审计，其受托技术责任属于受托财务责任的二级责任，比如 IT 审计中，保证会计报表真实可靠，就必须要求信息系统的软件系统和硬件系统同时可靠，后者从属于前者，被审单位承担的受托信息技术责任就是其所负受托财务责任的二级责任。在管理审计分支中的技术审计，其受托技术责任属于受托管理责任的二级责任。例如，环境审计实质是对环境管理的审计，因此属于管理审计。但进行企业环境审计，需要审查企业的生产工艺与生产技术，甚至审查产品的环保技术性能，此类技术方面的审计都是为了证实企业环境保护方面的受托管理责任。

总之，对财务会计的审计称为财务审计；对管理进行的审计称为管理审计；对技术方面的审计就应当称为技术审计。从这个意义上说，技术审计应是现代审计的第三大领域。20 世纪 30 年代以前财务审计一统天下，30 年代以后 80 年代以前管理审计异军突起，与财务审计并驾齐驱，80 年代以来技术审计不断涌现，90 年代IT审计初视端倪，21 世纪将是IT审计师独领风骚的时代。勿庸讳言，技术审计至今未能脱离财务审计和管理审计而单独存在。然而，尽管技术审计尚未独立

为现代审计的第三分支，但“技术审计”概念的提出仍然极具积极意义。技术审计反映了科技与审计、科技与经济管理相互融合与渗透的时代特点，要求审计人员既要掌握经济管理知识，又要掌握科学技术。现代审计向管理领域和技术领域渗透，是不以人的意志为转移的必然趋势。也许将来技术审计会成为与财务审计和管理审计相并列的第三大分支。

在不久的将来，无论是国家审计、内部审计还是注册会计师审计，不懂IT技术必然遭遇灾难性风险，离开IT审计将寸步难行。国际著名会计公司德勤会计师行的高级合伙人鲍威尔先生指出，全世界即将迎来管理领域信息化的高潮。信息技术对传统管理和控制的挑战是空前的，主要表现在三个方面一是内部控制环节的变化，许多传统的控制手段已经失去意义，评价和改进内部控制必须以信息系统的运转为基础；二是管理的风险增加，由于企业经营越来越依赖于信息系统，除了传统意义上的经营风险、控制风险和财务风险之外，企业信息系统安全性导致的信息技术风险日益增长；三是对复合性高级人才的需求骤增，要求管理者、审计师和咨询人员必须在精通管理和专业的同时熟悉信息系统和网络技术。

信息技术的发展对中国注册会计师和会计师事务所提出了更高的要求。国际同行的业务收入中，传统的财务审计服务所占收入比例正在迅速下降，风险控制服务和管理咨询服务收入的比重大大提高，而这些收入增长的部分往往又和IT环境审计、信息系统安全审计服务等技术性审计有关。可以断言在整个社会信息化程度迅速提高的今天，如果我国的会计师事务所不及早作好IT技术方面的人才准备，不仅谈不上和五大著名的国际会计师事务所竞争，而且连国内的市场也会丧失殆尽。

第2篇保险业IT内部审计

保险业IT内部审计保险行业上市公司不仅需要接受保监会的监督管理，而且还要面对公司发展和风险控制的内部需求。信息技术已经融入公司管理活动的各个方面，是保险行业各项管理职能的依托。

一、IT内部审计同IT治理和内部控制的关系

信息技术的重要性和复杂性使之影响到公司的决策及执行，IT 管理也表现出越来越严重的问题，主要表现在 IT 投资变得无法控制；风险控制与服务质量不能令其他部门满意；由于 IT 的专业性，IT 战略规划常常同公司总体战略难以协调，可能导致影响公司总体战略的贯彻执行。IT 治理就是为解决这些矛盾而引入的概念，现在 IT 治理已经在很多企业内实施，IT 治理是公司治理的一个关键部分，它能使企业合理利用 IT 资源，促使 IT 投资收益最大化，使得 IT 在复杂的管理环境下有效进行相关风险管理，从而保障 IT 服务质量，推动企业整体目标的实现。IT 内部审计是 IT 治理的重要组成部分，对 IT 治理起到促进作用。保险公司内部控制是指保险公司各层级的机构和人员依据各自的职责，采取适当措施，合理防范和有效控制经营管理中的各种风险，防止公司经营偏离发展战略的机制和过程。通过对内部控制的测评，确定系统信息的可依赖程度，评估控制风险的水平，减少审计工作量，节约审计成本，从而保障审计质量。内部审计是现代企业法人治理结构的内在需求，尤其是对于以经营风险为主的保险公司来讲，有效的内部审计对企业防范风险起到至关重要的作用。为有效节约审计成本，提高审计效率，外部审计也会使用内部审计工作成果。当然，两者在职能、地位、作用等方面都存在很大不同。内部审计部门是公司重要部门，内部审计是公司内部的一种独立、客观的监督和评价活动，它通过审查和评价经营活动及内部控制的适当性、合法性和有效性来促进公司总体目标的实现。内部审计人员需要熟悉公司保险经营和投资经营的运作流程，从整体上把握企业的经营管理。二、现阶段保险行业 IT 内部审计特点

顺应政府监管的要求保险行业上市公司除中国人寿在美国上市需要执行 SOX 法案之外，其他保险公司需要执行保监会《保险公司内部控制基本准则》第三十条中有关于信息技术控制的专门条款，《保险公司内部控制指导原则》第八章支持保障系统中的 48~53 条中关于计算机信息系统控制的要求。

技术标准的选择一般监管部门会就 IT 内部控制提出基本准则和指导原则，选择具体的审计标准来达到政府的监管要求是保险公司 IT 内

部审计需要解决的问题，现在有关 IT 内部控制和 IT 审计的国际标准很多，这些标准各具特点。一般保险公司的做法都是按照 COBIT 标准，根据自身特点，结合信息系统生命周期各个阶段的不同特点有选择性地实施 COBIT 控制模型，COBIT 将 IT 过程、IT 资源及信息与企业的策略、目标联系起来，形成一个三维的体系结构。其中，IT 准则反映了企业的战略目标，从质量、成本、时间、资源利用率、系统效率、保密性、可用性等方面来保障信息的安全性和有效性；IT 资源包括专业人才、应用系统、技术、设施及数据在内的信息相关的资源；IT 过程从信息技术的规划与组织、采集与实施、交付与支持、监控等四个方面，确定了 34 个信息技术处理过程。 IT 审计技术与方法该方法主要包括测试数据法、平行模拟法、嵌入审计模块法、虚拟实体法、受控处理法、受控再处理法和程序代码检查法。有效控制 IT 内部审计把对审计风险的检查控制作为 IT 内部审计的重要质量控制目标。审计风险分为重大错误风险和检查风险，由于 IT 系统复杂性，检查风险是客观存在的，为避免检查风险的出现需要对 IT 内部审计进行有效控制。

采用非现场审计的方式依靠强大的信息技术的平台，IT 内部审计主要采用非现场审计的

方式进行。通过远程方式对审计对象相关数据和资料的不断搜集、整理和分析，把审计由事后审计变为事前统一规范、事中监督预警、事后定期分析回顾的过程。三、保险业 IT 内部审计需要关注的问题

业务与 IT 联合审计 IT 内部审计与其他内部审计相比在技术上有其独特之处，如今 IT 和业务的融合越来越紧密，IT 在支撑业务同时，也利用新的技术手段引领业务发展。因而 IT 和业务也需要进行联合审计，交付给公司管理层一个统一、全面的审计结论，使得审计结果更好地服务于公司稳定发展的总体目标。

从公司治理结构上解决审计独立性问题如何加强内部审计的独立性一直是内部审计探讨的重点，现在很多保险公司 IT 内部审计独立性从组织结构上来说还没有得到彻底解决，成立有公司决策层参加的审计委员会、有独立于 IT 研发和运维 IT 内部审计机构以保障 IT 内控审计和实质性审计的客观公正，是 IT 内部审计独立性的必然要求。

提高 IT 内部审计人员比例和素质 IT 审计是 IT 技术和审计技术相结合的边缘学科，IT 审计人才是复合型人才，需要原来的 IT 技术人员和内部审计人员彼此钻研对方的学科，同时掌握财务、运营、商务等管理知识，在通过 CISA 认证的同时还需要有 CFA、CIA、CISP 等认证。人员素质的提高也是通过需求拉动的，只要公司有相应的需求和激励措施，人员素质的提高是指日可待的。

新技术和 IT 审计新理念、新技术的吸收运用新技术、IT 审计新理念、新技术层出不穷，新理念、新技术对提高生产力、拉动经济增长、改变生活方式等具有良好的促进作用。只有加强对新理念、新技术的了解，迅速做出应对，才能适应时代的发展变化。

处理好 IT 内部审计的关系一是 IT 内部审计与 IT 研发、运维、管理关系；二是调整好内部审计与社会审计、国家审计的关系；三是摆正 IT 内部审计在公司内部审计中的位置。

成本效益原则 IT 内部审计同样需要遵从成本效益原则，不能进行不计成本的投入，服务公司追求股东利益最大化的整体目标，在兼顾效益的原则下进行适度审计。

拓宽 IT 内部审计的范围 IT 内部审计经历了 EDP 审计，正处在信息系统安全性、可靠性、有效性的测试和评价的审计阶段，IT 内部审计需要向咨询审计的方向发展，致力于 IT 治理结构和管理流程的改进，告诉公司管理层应该如何做才能符合公司总体发展的利益，改变 IT 内部审计在公司相对弱势的地位，依靠工作成果来加强巩固 IT 内部审计在公司的地位。规范 IT 内部审计体系参照监管部门提出的监管要求、IT 内部控制和 IT 审计的国际标准，编写发布更适应各保险公司自身情况的《IT 内部审计准则》和具体指导 IT 内部审计工作的《IT 内部审计指南》等 IT 内部审计规范性文件，开发 IT 内部审计工具和 IT 内部审计 MIS 系统，通过规范自身的 IT 内部审计体系来规范 IT 内部审计行为、保障 IT 内部审计的质量和效果。如今，观念和技术的创新是发展的主旋律，IT 在保险公司的广泛应用更需要 IT 内部审计的保驾护航，IT 内部审计在保险行业处于曙光乍现、借力待发的阶段，必将促进保险公司按照既定目标健康有序的发展，也并将随着保险这个朝阳产业

第 3 篇公司层面 IT 审计

1、ITELC介绍 IT 控制环境 IT 风险评估 IT 信息与沟通 IT 监控

公司的 IT 组织架构是如何设定的？ ?公司的 IT 战略规划是如何设定的？

公司的 IT 组织架构及战略规划是否与企业整体相适应？ ?公司是否对 IT 风险进行评估？

公司是否对 IT 风险进行了有效的管理？ ?公司是否制定了适当的 IT 政策及制度？ ?IT 政策及制度是否被定期审阅并更新？ ?IT 政策及制度是否与员工进行了沟通？ ?管理层如何对 IT 活动进行监控与评估？ ?内审部门是否拥有进行 IT 审计的资源？ ?内审计划中是否包括 IT 审计的内容？

1、ITELC介绍 ELC-E1 控制目标

企业的 IT 战略规划、计划及预算等与企业的整体战略规划及业务目标相一致。标准控制活动

企业相关职能部门制定了与企业整体战略规划及业务目标相一致的 IT 战略规划、IT 年度计划及预算，并且得到了管理层的批准。测试步骤

1、询问 IT 部门领导，了解公司 IT 战略规划、IT 年度计划和 IT 年度预算的制定、审批及下发流程。

2、获取并检查公司 IT 战略规划、IT 年度工作计划及 IT 年度工作预算，确认公司是否制定了与企业整体战略规划及业务目标相一致的 IT 战略规划、IT 年度计划及预算；

3、获取 IT 战略规划、IT 年度工作计划及 IT 年度工作预算的审批文档（可能是由公司 IT 治理委员会审批记录，也可能是公司董事长或总经理的签批文件），确认上述文档是否经过管理层的审批。

证据示例战略规划工作计划 3 .预算审批文件审批文件审批文件

ELC-E1 控制目标

IT 部门机构设置合理，并配备具有适当技能和经验的人员。标准控制活动

IT 指导委员会及独立的信息技术部门，并根据职责分工情况设置了合理的科室和人

员岗位，对各岗位人员职责、能力明确定义和说明，并确保职责分离。测试步骤

1、询问 IT 部门领导，了解公司 IT 指导委员会（其他叫法包括 IT 治理委员会、IT 科技委员会、

IT 战略管理委员会等）及 IT 部门的职能设置和人员配备情况。 2、获取并查看 IT 指导委员会的组织架构和职能说明，确认公司 IT 指导委员会设置是否合理；获取并检查 IT 指导委员会会议纪要，确认 IT 指导委员会是否按照公司要求履行其职能。（如果

公司 IT 环境比较简单，没有成立 IT 指导委员会，可以直接对 IT 部门的设置进行测试。）3、获取并查看 IT 部门的组织架构图以及岗位说明书，确认公司是否合理设置了 IT 部门和员工

岗位，并对岗位人员的职责进行了明确定义和说明，且确保职责分离。

ELC-E1 控制目标

企业对 IT 风险进行有效评估及管理。标准控制活动

企业建立了合乎规范的 IT 风险评估机制，包括评估方法、评估机构人员安排、评估报告等，并针对不同的风险设计了必要的应对措施。测试步骤

1、询问 IT 部门领导，了解公司是否积极进行持续性的风险评估，并将其作为设计和执行内部控制，定义 IT 策略以及监控评价机制的一个重要手段；

2、获取并检查 IT 风险评估体系文档及审计年度内的 IT 风险评估报告，确认公司是否制定了

合乎规范的 IT 风险评估机制并定期开展 IT 风险评估工作。

ELC-E1 控制目标

IT 部门与其他部门有效沟通，满足其业务需求。标准控制活动

企业设立了专门委员会或专门的协调机制保证业务部门与 IT 部门就具体业务需求充分沟通，保证各部门行动协调一致。测试步骤

、询问IT部门领导，了解公司是否建立了专门的协调机制以确保业务部门与IT部门就具体业务需求进

行充分沟通（如是否建立了专门的管理委员会、是否定期召开跨部门会议等）。

2、根据IT部门与业务部门的实际沟通机制，按照财务审计/ITA抽样原则确认样本量，获取并检查其沟

通交流的相关证据资料（如会议纪要，来往邮件等），确认公司是否建立了专门的协调机制以确保业

务部门与IT部门就具体业务需求进行充分沟通。

ELC-E1 控制目标

IT 制度被及时下发并遵照执行，避免 IT 资产及信息损失。标准控制活动 IT 部门订立了信息系统使用规范，并使用适当的渠道下发至有关业务部门，同时举办相关培训，以确保

业务部门了解并执行信息系统使用规范。测试步骤

1、询问IT部门领导，了解公司是否制定了信息系统使用规范，是否使用适当的渠道下发至有关业务部

门并举办相关培训。

2、获取并检查相关信息系统使用规范，确认公司是否制定了信息系统使用规范。

3、按照询问得知的下发渠道，获取并检查信息系统使用规范下发平台截图或其他证据（如内网、员工手册、OA 系统等），确认公司是否通过适当的渠道将信息系统使用规范下发至有关业务部门；

4、获取并检查信息系统使用规范培训相关证据（如培训计划、培训通知、培训资料、签到表等），

确认公司是否对员工进行信息系统使用规范的相关培训。

ELC-E1 控制目标

IT 部门内部管理制度完善，IT 人员受到必要的专业培训。标准控制活动

企业建立了针对IT部门及IT人员的各项管理制度，并安排必要的培训，使IT人员了解这些制度，并具备