注册信息系统审计师考试介绍及应试对策

□ 史振生 张爱芹

随着信息技术在财务会计、管理领域应用程度的不断提高，信息系统审计业务也逐渐受到职业会计师行业的重视。在我国，信息系统审计业务的开展还处于探索阶段。其实，信息系统审计在国外已经有了一个相当长时期的发展，而且也产生了相应的专业组织和专业资格。信息系统审计与控制协会(ISACA)就是从事计算机审计人员(IT审计师)组成的国际性专业组织，由该组织颁发的信息系统审计师(CISA)资格也是这一领域唯一的受国际认可的专业资格。

一、注册信息系统审计师(CISA)背景资料

1、什么是信息系统审计师

注册信息系统审计师（Certified Information System Auditor，简称CISA）是指既通晓信息系统的软件、硬件、开发、运营、维护、管理和安全，又熟悉经济管理的核心要义，能够利用规范和先进的审计技术，对信息系统的安全性、稳定性和有效性进行审计、检查、评价和改造。

2、现代社会为什么急需信息系统审计师

21世纪是信息化的时代，生产、交易和管理都离不开信息流和对信息流的管制，管理人员在面对传统经营风险和财务风险的同时，必须随时面对信息风险对企业生存和发展的挑战，人们不难想象，假如银行的存贷款数据库被黑客破坏，假如证券交易所的信息系统突然崩溃，假如企业ERP系统中的应收账款模块产生混乱，假如仓库的自动订货和发货系统无法修复，我们面对的将不单单是损失，而是破产、混乱和崩溃！

3、信息系统审计师关注的问题

顺应时代要求，信息系统审计师将在信息化社会中，为各单位筑起一道信息安全的壁垒。他们关注的问题主要有：

(1)信息安全。没有安全就没有一切，信息系统审计师会采用各种方法来测试系统的安全性，并对来自内部和外部的安全隐患提出相应对策；

(2)信息系统的稳定性。没有长期稳定性，信息系统就无法承担起激烈竞争的压力，信息系统审计师会提出一系列对策保证客户信息系统的万无一失。

(3)鉴别信息系统的有效性。最安全和最稳定的系统不一定是最有效的系统，而效率不高的系统会消耗企业大量的资源，信息系统审计师的优势就是对财经管理和信息技术融会贯通，为企业信息系统的改造提供建议。

4、哪些行业最需要信息系统审计师

软件供应商。特别是经济管理类的集成软件供应商，需要信息系统审计师参与产品设计、规划和检测，需要信息系统审计师对客户现有信息系统进行评价，提出改造设想。全球所有重要的ERP和CRM产品供应商都聘请大量信息系统审计师。

管理咨询机构。20世纪90年代以后，管理咨询的重点已经逐步发展为提供一揽子解决方案，其中信息系统的配置，就是解决方案成功的基础。国际知名的管理咨询机构中，有50%以上的员工熟悉信息技术，其中20%拥有信息系统审计师资格。

会计师事务所。这是信息系统审计师最早的落脚点。“五大”国际会计公司超过30%的收入来自于风险管理部门。这个部门的最主要工作就是监控客户的信息系统风险和运营风险，同时为客户提供ERP或CRM的安装、维护和培训。会计师事务所中传统财务报表审计也越来越离不开信息系统审计师的贡献，没有他们的工作，评估内部控制风险和企业固有风险将成为一句空话。

跨国公司。作为信息系统最集中的用户，跨国公司急需大量信息系统审计师，一方面参与信息化建设的过程，另一方面时刻保持对分支机构的信息监控。最新迹象表明，跨国公司内部审计部门也在大量招聘信息系统审计师，以加强内部的监督和牵制。

大型国有企业和上市公司。这些机构往往有雄厚的财力来实现管理的信息化、保证生产经营的稳定性，他们对信息系统审计师的要求和跨国公司类似。

5、谁有资格授予信息系统审计师资格

目前国际上，信息系统审计与控制协会ISACA(Information System Audit and Control Association)是唯一有权授予国际信息系统审计师资格的跨国界、跨行业专业机构，该协会成立于1969年，最初称为EDP审计师联合会，总部在美国的芝加哥。目前在世界上100多个国家设有160多个分会，现有会员两万多人。注册信息系统审计师资格由ISACA授予，是信息系统审计领域的唯一职业资格，得到全世界的广泛认可。

6、取得CISA资格的条件

通过CISA考试；在信息系统审计、控制、或安全领域5年的工作经验；遵守ISACA的职业道德；提出CISA资格申请并得到批准。

7、考试日期、时间、地点和国内组织单位

国际上CISA考试每年6月组织一次，考试时间为4个小时。目前国内从事CISA考试组织培训工作的单位是国家审计署干部培训中心，该中心确定的国内考试地点为上海、武汉、北京、深圳、成都等地。CISA考试题型为200道客观选择题，全部为笔答，满分100分，75分及格。考试语言主要是英文，目前还没有中文考试。

二、CISA考试内容及应试对策

CISA考试要求应试者具有扎实的审计理论和审计实践经验，具有较丰富的企业运营及管理知识和经验，同时更要具有全面的、有一定深度的计算机信息系统方面的理论和实践经验。CISA考试分为信息系统审计和信息系统相关知识两个方面七大内容：

1、信息系统审计程序(10%)

(1)考核要点。实施信息系统审计要与一般公认的信息系统审计标准和准则相一致，以确保对组织采用的信息技术和业务系统进行充分的控制、监控和评价。主要包括：审计计划和审计战略及目标；一般公认的审计标准；信息的收集和分析；风险管理和控制等。

(2)应试对策。这部分考试涉及的主要知识有：有关信息系统审计的标准和准则；审计实务和技术；风险分析方法、原则和标准；战略和计划过程；信息系统及技术发展趋势；质量管理、财务管理和业务管理等。

考生必须具备现代审计理论和实务、企业管理、项目管理和信息系统及信息技术发展脉络方面的知识。

2、信息系统的管理计划和组织(11%)

(1)考核要点。评价有关信息系统管理、计划和组织的战略、政策、标准、过程和有关实务。主要包括：评价信息系统战略和过程；评价信息系统政策、标准和过程的开发、部署和维护；评价信息系统组织和结构等。

(2)应试对策。这部分考试涉及的主要知识有：有关信息系统战略、政策、标准和过程的主要实践；信息系统战略开发、部署和维护的方法和步骤；信息系统项目管理、风险管理、变动管理、质量管理、安全管理；信息系统组织结构和设计原则；软件质量管理等。

考生必须具备信息系统开发与管理、项目管理及软件工程方面的知识。

3、技术基础和操作实务(13%)

(1)考核要点。评价组织技术和操作基础的实施及正在进行的管理的功效和效率，确保它们充分地支持组织的业务目标。主要包括：评价硬件的取得、安装和维护；评价系统软件和应用软件的获取、实施及维护；评价网络基础设施的获得、安装和维护；评价信息系统操作实务；评价系统执行和监控过程、工具和技术等。

(2)应试对策。这部分考试涉及的主要知识有：有关硬件平台、系统软件和实用软件以及网络基础设施和信息系统操作实务的风险和控制；系统运行和监控过程、工具和技术；IT基础设施的获取、开发、实施和维护的过程；网络拓扑等知识。

考生必须具备一定的计算机硬件和软件、计算机网络(尤其是互联网等)基础和运行管理等方面的知识。

4、信息资产的保护(25%)

(1)考核要点。评价逻辑的、环境的和IT基础设施的安全，确保系统满足组织的业务需求，保护信息资产以防非授权使用、泄露、修改、破坏和损失。主要包括：评价逻辑访问控制的设计、实施和监控；评价网络基础设施的安全；评价环境控制的设计、实施和监控；评价物理访问控制的设计、实施和监控等。

(2)应试对策。这部分考试涉及的主要知识有：计算机访问控制原理和技术；物理安全控制；密码技术；网络安全概念；安全体系结构；安全评估工具；病毒及探测、预防和反应机制；黑客攻击方法和技术等。

考生必须具备扎实的计算机网络理论知识和实践经验、计算机加密解密技术、计算机病毒及网络黑客技术、计算机及网络安全体系结构方面的知识等。

5、灾难恢复和业务持续计划(10%)

(1)考核要点。评价在系统发生不测时，为使业务运转和信息系统处理能正常进行，而采取的备份和恢复等措施。主要包括：文件及数据的备份和恢复机制；不测发生后保证组织业务持续进行和继续提供信息系统处理的能力等。

(2)应试对策。这部分考试涉及的主要知识有：关于灾难恢复和业务持续的概念和方法、灾难恢复和业务持续技

术等。

考生必须具备数据库理论中关于数据恢复技术和灾难应对措施方面的知识。

6、业务应用系统的开发、取得、实施和维护(16%)

(1)考核要点。通过业务应用系统的开发、取得、实施和维护来评价采用的方法和过程，以确保与组织的业务目标一致。主要内容包括：对应用系统的开发、取得、实施和维护中采用技术和方法进行评价。

(2)应试对策。这部分考试涉及的主要知识有：系统开发方法和工具；软件质量保证方法；程序设计原理和技术；系统实施后的评价技术等。

考生必须具备软件工程的理论及实务、各种程序设计技术、信息系统实施和评价等方面的知识。

7、业务过程的评价和风险管理(15%)

(1)考核要点。评价业务系统和过程，确保风险被控制且与组织业务目标相一致。主要内容包括：通过诸如用基准测试程序测试、最优方法分析、业务流程重组(BPR)，评价信息系统支持业务过程的效率和效力，确保业务结果最优；评价自动化和手工控制的设计和实施；评价组织的风险管理和控制的实施等。

(2)应试对策。这部分考试涉及的主要知识有：最优方法业务过程；业务过程控制；业务设计机构、管理和控制实务；业务流程设计、重组和改进的方法等。

考生必须具备企业管理、企业生产经营和电子商务方面的理论及实务知识。

(作者单位：河北经贸大学
会计学院)

责任编辑 王教育

□ 石钟韶

ERP(企业资源计划系统)进入中国已有十几年的历史，但是ERP概念在中国深入人心却是最近几年的事情。随着中国加入WTO企业信息化的需求越来越迫切，再加上ERP厂商一轮又一轮的宣传攻式，很多企业或被动或主动地接受了ERP的改造。但是，作为一种在国外已经有数十年发展历史的管理概念，ERP在现代企业管理中已经越来越显得力不从心。ERP在实际应用中暴露出的越来越多的问题，迫使我们不得不重新思考，ERP是否真是一剂灵丹妙药？中国企业及财务管理信息化在理想和现实之间到底还差多远？

ERP 问题——理想和现实的差距

“上ERP是找死，不上ERP是等死”。“联想”柳传志这句广为流传的名言生动地描述了企业应用ERP系统的矛盾心理。在信息时代，企业需要先进的管理方式，技术和管理理念的结合是不可避免的大趋势，ERP正是顺应这一潮流应运而生的。但是，在经过了多年的发展之后，ERP的应用也遇到了前所未有的困难，ERP的理论渐渐开始落后于时代。

目前看来，中国的ERP至少面临三大问题：首先是ERP厂商自身的问题。国外ERP产品在理念、模式和技术上有其先进性和成熟性，但国外厂商往往不了解中国企业的实际情况，同时实施成本高昂，项目风险太大。国内ERP软件供应商凭借着对中国国情的了解，能提供更加本地化的服务，但是在技术、经验和应用实践上还显稚嫩。其次，实施成本和周期的问题也给企业带来了比较大的风险，一旦不成功代价惨重，令很多企业望而却步。即使是堪称国内ERP应用楷模的IT企业“联想”，也有柳传志发出“九死一生”的感慨。其他传统型的中国企业要上ERP的难度可想而知。最后，随着时代的发展，企业内外部情况发生着错综复杂的变化，市场条件、竞争机制甚至商业原理都和传统的经济理论有很大的不同。在这种情况下，ERP的管理思想已经很难正确地分析企业资源和市场之间的关系，这也是导致很多ERP项目与实际工作脱节的重要原因。