Mc Graw Hill Education

中国IT治理·价值丛书

IT审计（第二版）

管好信息资产

IT AUDITING

USING CONTROLS TO PROTECT INFORMATION ASSETS

〔美〕克里斯·戴维斯
〔美〕麦克·席勒 著
〔美〕凯文·惠勒
农信银资金清算中心有限责任公司 审
中治研（北京）国际信息技术研究院 译

中国经济出版社
CHINA ECONOMIC PUBLISHING HOUSE

IT审计（第二版）

管好信息资产

IT AUDITING

USING CONTROLS TO
PROTECT INFORMATION ASSETS

〔美〕克里斯·戴维斯
〔美〕麦克·席勒 著
〔美〕凯文·惠勒
农信银资金清算中心有限责任公司 审
中治研（北京）国际信息技术研究院 译

中国经济出版社
CHINA ECONOMIC PUBLISHING HOUSE
北京

图书在版编目（CIP）数据

IT 审计：管好信息资产（第 2 版）/（美）克里斯·戴维斯（Davis，C.），（美）麦克·席勒（Schiller，M.），（美）凯文·惠勒（Wheeler，K.）著；中治研（北京）国际信息技术研究院 译.

北京：中国经济出版社，2015.4

ISBN 978-7-5136-3599-8

Ⅰ.①I… Ⅱ.①戴… ②席… ③惠… ④中… Ⅲ.①信息系统—审计 Ⅳ.①F239.6

中国版本图书馆 CIP 数据核字（2014）第 2819984 号

Chris Davis，Mike Schiller，Kevin Wheeler

IT Auditing：Using Controls to Protect Information Assets，2nd Edition

ISBN：0-07-174238-7

责任编辑　潘　静

责任审读　霍宏涛

责任印制　巢新强

封面设计　华子图文设计公司

出版发行　中国经济出版社

印 刷 者　北京科信印刷有限公司

经 销 者　各地新华书店

开　　本　710mm×1000mm　1/16

印　　张　34.5

字　　数　480 千字

版　　次　2015 年 4 月第 1 版

印　　次　2015 年 4 月第 1 次

定　　价　108.00 元

广告经营许可证　京西工商广字第 8179 号

中国经济出版社 **网址** www.economyph.com **社址** 北京市西城区百万庄北街 3 号 **邮编** 100037

本版图书如存在印装质量问题，请与本社发行中心联系调换（联系电话：010-68330607）

总 序

从电子计算机到国际互联网再到物联网、大数据，我们这代人经历了一个人类历史上非常特殊的时代，大家称之为IT革命和信息化时代。这个时代的特点是生产数字化、生活信息化、金融电子化、教育网络化、文化多元化、经济全球化、全球一体化。

这样一种社会形态在人类历史上前所未有。人类社会像脱缰的野马，以前所未有的速度奔向未来。事实上，从另一个角度看，人类已进入高度依赖IT的时代。

现代社会的人们已不能想象一个没有信息科技的环境，同时信息科技风险无时不在，所以信息科技治理十分必要。

我在金融系统工作多年，亲身经历了我国金融信息化建设。30多年来，经过金融人艰苦不懈努力，金融信息化工作取得了举世瞩目的成就，对推动我国经济和金融快速发展发挥了巨大作用，为国民经济转型和小康社会建设发挥了重要作用。金融信息系统不仅成为金融机构的业务运营、业务创新的基础平台，而且也是现代中国社会生产生活的重要组成部分。

当前，我国金融业面临着新的发展机遇与任务，也存在着新的风险与挑战。在这一重要战略机遇期，金融系统既要为我国经济转型和小康社会建设保驾护航，也要实现金融系统自身持续稳健经营、安全运行、提升核心竞争力的目标。这需要进一步加强战略规划，深化内部控制和风险管理，转变经营理念、管理机制和发展模式；优化IT治理结构，进一步提升信息科技发展水平将成为实现这一战略的重要手段；通过树立“科技引领”理念，促进信息科技与业务

发展的深度融合，增强可持续发展能力，为社会公众提供更丰富、安全和便捷的多样化金融服务。

中治研（北京）国际信息技术研究院院长陈天晴先生，长期在人民银行科技部门工作，具有丰富的金融科技工作经验。他组织编译一批先进实用的信息科技管理工具书（“中国IT治理·价值丛书”），不仅金融系统需要，其他行业也很需要。这套丛书汇集了从董事会、高管层、IT部门、业务部门、监管部门等多视角的观念和需要，同时也包含了IT目标、组织架构、IT规划、IT投资及价值、风险管理和审计、外包管理、云服务、数据中心、灾难恢复、IT服务管理等具体实践的方法。希望这套丛书能够成为IT治理研究者和实践者，特别是企业科技部门主管的得力助手，成为企业高管层的参考书。

苏宁

中国人民银行原副行长

指导委员会名单

（以姓氏笔画排序）

于　玫　于　进　王永红　陈　波　陈文雄　余　彤
李春亮　杨　竑　张　野　林晓轩　金磐石　侯维栋
胡红升　柴洪峰　曹少雄　谢翀达　葛一苗

编委会顾问名单

（以姓氏笔画排序）

印甫盛　陈　进　陈　静　陈伟钢　陈文放　陈正清
吴树森　单怀光　恽铭庆　施雨农　唐世渭

编委会名单

主　任：陈天晴

副主任（以姓氏笔画）：

王云生　王申科　王耀辉　叶又升　史晨阳　朱宏玲
陈　静（女）　张　胜　张　艳　汪国强　梁　峰

委员（以姓氏笔画）：

于　锋　马　庆　尤进伦　王东红　王成涛　方渝军
刘永成　刘述忠　左　川　白　锘　孙卫东　吴　萌
张海彤　苏宝华　肖　政　苏　云　李长征　周正明
杨晓平　赵成刚　洪　浩　胡秀红　姚晖晖　段青松
程晓阳　韩兆云　曹　艳　闫振平　裴恒亮　杨红江
陈划生

翻译（以姓氏笔画）：

卢玉婷　李志平　李　芳　苗　博　杨　峰　姜　冰
秦思思　佟文华

IT 审计（第二版）评述

本书旨在指导和帮助审计人员对控制环境和残余风险的范围进行正确评估。作者将复杂的代码格式用简单易懂的叙述方式向读者展示出来，给予读者思想上的启迪和行动上的鼓励。

——库尔特·罗莫（Kurt Roemer）
思杰首席安全战略师

本书详细阐述了在复杂的信息化环境中开展 IT 审计的有效方法，是一本审计人员和 IT 管理者必备的教科书。

——肖恩·艾文（Shawn Irving）
西南航空信息技术部高级经理，负责 IT 安全标准与验证

传统 IT 审计主要利用企业型工具对企业系统进行集中处理。但是，当企业系统开始面向外包和云基服务时，这些分布式系统则需用新的云基工具进行审计。企业外包商要么重写代码，要么利用已有的或新的云基工具，帮助审计人员审计分布式系统。本书在如何应对 IT 云基服务审计中所面临的新挑战方面给予了读者一些意见。

——马修 R. 阿尔德曼（Matthew R. Alderman）
科利斯产品管理公司董事，信息系统安全认证专家

本书作为 IT 审计人员的必读书，在虚拟计算环境下应对信息系统安全防范方面做出了重要的贡献。

——彼得·巴希尔（Peter Bassill）

盖勒考罗集团首席信息安全官，注册信息技术专家
信息系统审计与控制协会安全顾问团安全认证专家

过去的几年里，我的本科学生在IT审计与风险管理课程中所使用的教材正是《IT审计》(第一版)。虽然学生的背景各不相同，但都觉得此书非常受用。如今，知悉该书第二版中收录了针对云计算和虚拟环境等新内容并出版，我们感到非常的兴奋。本书作者能准确把握IT风险管理的实质，能针对不同知识水平的人群做到因材施教。

——马克·萨拉玛西科（Mark Salamasick）
得克萨斯州立大学，达拉斯管理学院内审中心主任

《IT审计》(第二版) 有很多优点，如内容涵盖全面、结构设计合理、表述通俗易懂、解释清晰详尽，同时给出很多对IT审计人员有用的建议。本书确实是一本不可多得的好书，特别是对于那些涉猎行业前沿的从业人员来说，是非常有用的。

——马克·文森特（Mark Vincent）
盖勒考罗集团信息安全官，信息系统安全认证专家

致我亲爱的妻子萨拉（Sarah）及我可爱的三个孩子，乔休尔（Joshua）、卡勒（Caleb）和凯尔西（Kelsea）：

为了此书的成功出版，我们聚少离多。然而，正是你们对我的理解和支持，才有今天的成就。谢谢你们！

——爱你们的克里斯（Chris）

致我亲爱的斯蒂芬妮（Stephanie）、格兰特（Grant）和凯特（Kate）：

没有你们的耐心、理解和支持，最重要的是你们对我的爱，此书不可能一蹴而就，善始善终。我为每一天你们带给我无比的快乐和幸运而感到万分荣幸。

——麦克（Mike）

作者简介

克里斯·戴维斯（Chris Davis），工商管理硕士（MBA）、注册信息系统审计师（CISA）、信息系统安全认证专家（CISSP）、思科认证网络高级工程师（CCNP）。曾应邀为政府、企业、高等院校的IT人员进行信息安全、计算机取证、硬件安全设计、IT审计和认证课程方面的讲座和培训。是《黑客大曝光之计算机取证》2009版和2004版（*Hacking Exposed Computer Forensics* 2009，2004）、《反黑客工具包》2006版和2003版（*Anti-Hacker Toolkit* 2006，2003）以及《IT审计》2006版（第一版）（*IT Auditing* 2006）的作者之一。同时参与了《网络数字犯罪与鉴侦科学》（*Digital Crime and Forensic Science in Cyberspace*）和《计算机安全手册》（第五版）（*Computer Security Handbook*，5th Edition）的编写工作。参与过诸如PCI－SSC虚拟化特别兴趣小组、信息系统审计与控制协会、Spice World、SANS、高德纳公司、哈佛、黑帽、CEIC和全球移动通信3G网络等的IT治理项目。

克里斯本科毕业于托马斯爱迪生州立学院（Thomas Edison State College）核工程技术专业，随后获得得克萨斯大学（University of Texas）工商管理硕士学位，辅修信息安全课程。毕业后曾在美国海军潜艇舰队服役8年，分别在美国海军“特务”NR－1潜艇和内布拉斯加号弹道导弹核潜艇上服役。现为南卫理公会大学（Southern Methodist University）客座教授，同时在精数系统（Accudata Systems）、福瑞斯考特（ForeScout）和德州仪器（Texas Instrument）等公司兼职从事IT治理工作。

麦克·席勒（Mike Schiller），注册信息系统审计师（CISA），从事IT审计工作15年。曾任南卫理公会大学（Southern Methodist University）IT

审计课程讲师，经常受邀在CACS、信息安全世界（InfoSec World）和全美用户协会（ASUG）等大会上就相关内容发表演讲。现任德州仪器全球IT审计总监、世博集团IT审计总监，主要负责IT运营，服务器、数据库和存储设施运维，同时牵头负责数据中心、IT资产管理、帮助平台、网络应用和PC等多部门业务。

麦克毕业于德州农机大学（Texas A&M University）商情分析专业。工作之余，他喜欢观看棒球比赛，同时每年作为运动员参加美国全民棒球联赛。麦克是德州奇侠队和辛辛那提红人队的忠实粉丝。麦克的儿子（格兰特）是美国知名的棒球博主，曾荣获2005年德州奇侠队年度最佳球迷荣誉称号。麦克的女儿（凯特）则是当地小有名气的艺术家。麦克还创办了自己的教会——理查德森东基督教会。

其他作者

史黛丝·哈梅克（Stacey Hamaker），注册信息审计师（CIA），注册信息系统审计师（CISA）。现任美国三叶技术公司总裁，专门为世界500强企业、中小型企业和其他公共事业单位及部门提供企业级IT咨询服务。史黛丝是2002年《萨班斯－奥克斯利法案》（the Sarbanes－Oxley Act of 2002）的起草人之一，信息系统审计与控制协会北得克萨斯分会（the North Texas chapter of ISACA）委员，国际内部审计师协会（the Institute of Internal Auditors）会员。她经常受邀在全国各地以及国外的行业大会上发表演讲，并且为《信息系统控制杂志》撰写过多篇有关企业管理和IT治理的文章，在业内掀起了不小的反响。史黛丝女士本科毕业于美国俄亥俄州马瑞埃塔大学（Marietta College）会计专业，随后获得得克萨斯大学（University of Texas）工商管理硕士学位，辅修信息系统管理课程。

亚伦·纽曼（Aaron Newman），应用安全公司（Application Security, Inc.）创始人兼首席技术总监，全球最出色的数据库安全专家。亚伦曾为甲骨文公司（Oracle）参与编著《甲骨文安全手册》，并且他持有诸如数据

库加密与监测等多项技术专利。在成立 AppsecInc 之前，他还创办了其他的科技公司，如被誉为数据库安全漏洞评估先锋的 DbSecure 公司和被誉为数据库安全咨询翘楚的埃森哲软件系统公司。在过去十年里，亚伦先生一直致力于数据库安全解决方案的研究、设计和管理工作，特别是对数据库漏洞安全和相关市场开拓方面做出了巨大贡献。同时，亚伦受聘于诸如普华永道（Price Waterhouse）、互联网安全系统公司（Internet Security Systems）、入侵检测公司（Intrusion Detection Inc.）和银行家信托集团（Banker's Trust）等多家公司担任技术顾问。

凯文·惠勒（Kevin Wheeler），注册信息系统审计师（CISA）、信息系统安全认证专家（CISSP）、美国国家安全局 IAM/IEM。信息安全咨询公司——信息系统防御公司（InfoDefense）创始人兼首席执行官。凯文曾供职于美国银行（Bank of America）、电子数据系统公司（EDS）、迈克菲（Mcafee）、南卫理公会大学（Southern Methodist University）和德州政府（the State of Texas）。经常受邀为政府和商业机构做信息安全审计与评估、信息安全设计，计算机突发事件应急、商业策划和 IT 安全等 IT 治理相关咨询。服务领域涉及金融、卫生和 IT 行业，并且是信息系统安全协会（ISSA）、信息系统审计与控制协会（ISACA）、Infragard、北德州预防电子犯罪工作组（the North Texas Electronic Crimes Task Force）和大达拉斯商会（Greater Dallas Chamber of Commerce）的会员。凯文毕业于贝勒大学（Baylor University），获企业管理学士学位。

第二版技术审核人员

迈克尔·考克斯（Michael Cox），信息系统安全认证专家（CISSP）。现任德州仪器网络安全工程师，同时负责公司 IT 审计项目和工具研发。迈克尔曾经作为北电网络（Nortel）的网络工程师从事 Linux 系统管理工作。他毕业于艾柏林基督大学（Abilene Christian University）历史专业。曾任《IT 审计》第一版的技术审核专家。

麦克·库里（Mike Curry），注册信息系统审计师（CISA）。在德州仪器工作的15余年，有12年的时间一直在从事IT内审工作。作为高级IT审计师，他主要负责对操作系统、数据库、网络、应用系统和相关程序进行内部控制和安全审计，同时对相关法律遵从进行评估。

威绍尔·曼赫拉（Vishal Mehra），高级技术专家。在德州仪器工作10余年，负责过诸如网站应用研发、应用/基础设施构架和全球基础设施运营等多个部门的工作。现在主要负责服务器、存储、数据库的管理及操作系统、存储、虚拟化和数据保护的战略制定工作。威绍尔毕业于休斯顿大学计算机科学专业，获理学硕士学位。

第一版技术审核人员

芭芭拉·安德森（Barbara Anderson），思科认证安全专家（CCSP）、思科认证网络专家（CCNP）、思科认证网络设计专家（CCDP）。从业12年，在IT网络和服务器安全领域具有丰富的经验。作为高级网络安全工程师，芭芭拉有着深厚的专业背景知识和多年为企业提供网络和安全设计、执行及生命周期管理的咨询和服务经验。她曾在美国空军服役4年，之后先后供职于EDS、SMU Fujitsu、ACS和Fishnet Security。所有这些工作经验使她逐渐成为企业安全、产品配置和培训方面的IT专家。

蒂姆·布里丁（Tim Breeding），注册信息系统审计师（CISA），国际企业咨询治理师（CGEIT）。曾在德州仪器任职13年，期间负责公司计算机运行、软件开发测试和IS审计工作。之后又进入西南航空工作，在其供职的6年时间里，公司IS审计部门在他的领导下得到了长足的发展。再后来，蒂姆作为沃尔玛公司信息系统审计部门主管，主要对IT审计与咨询进行监督，制定风险评估及应对措施。现任沃尔玛转换系统部门高级主管，主要负责全美软件开发生命周期并积极推进用户接受重大变革系统。

苏伯士·高斯（Subesh Ghose），在德州仪器工作 13 年，从事多项 IT 治理工作。最初负责 IT 审计，对不同的数据中心、ERP 实施和基础设施环境进行内部控制，同时针对不同的技术平台和项目提出审计设计和实施方案，从项目开始阶段就介入内控机制。之后，主管 IT 安全和安全基础设施。负责对架构/流程进行研发，以保证外部合作机制和企业项目安全管控及德州仪器 ID 管理系统的正常运行。现在德州仪器全球生产运行部负责基础设施支持工作。苏伯士毕业于美国南方大学（Southern University）计算机科学专业，获理学硕士学位。

凯斯·罗伊德（Keith Loyd），信息系统安全认证专家（CISSP）、注册信息系统审计师（CISA）。曾在银行业工作 7 年，为银行法律业务系统提供技术支持，负责网络、应用系统、数据库和层级式入侵监测系统等的相关工作。在加入德州仪器之前，他还主要从事新应用的测试和漏洞监测、全球突发事件应急处置和国内市场调查等工作。凯斯获得卡佩拉大学（Cappella University）信息技术专业学士学位和诺维奇大学（Norwich University）信息安全专业硕士学位。

序言

在阅读这本书的时候，特别是当我看到作者能够在第一版的基础上不断探究、不断积累，对许多 IT 审计方面的新议题和内容能够做到与时俱进、推陈出新，我倍感欣慰，难抑激动之情，想趁此机会就 IT 审计的历史沿革向大家做个介绍。

纵观历史，拉丁语和法语对英语发展发挥过重要作用，英语“审计（audit）”一词即可追溯到拉丁语的“auditio”（意为“听、听取”）和法语的“auditre”（意为“听得见的”）。在 18 世纪以前，“audit”一直被定义为“向他人报告商业情况”，似乎“审计”更多指向结果。自从东印度公司（East India Company）和哈德逊湾公司（Hudson's Bay Company）等许多大型贸易合伙制公司出现之后，公司所有人和融资人才转向关心自己的投资是否安全。到了 19 世纪，铁路、船运、蒸汽机和大型工业逐渐兴起，但情况并不是太好，英国的许多铁路建设中途就停止了。投资人都想搞清楚到底发生了什么，是什么原因导致修建铁路的失败，他们投资的资金是否安全。同一时期，威廉·韦尔奇·德勤（William Welch Deloitte）创办了会计公司，并以自己的名字命名，专业代理铁路破产会计审计业务。之后德勤经历了多次并购。

400 多年前，世界上出现了最早的手写复式记账方式，与现代会计非常相似。没过多久，一个名叫赫尔曼·霍尔瑞斯（Herman Hollerith）的人发明了卡片编码系统，即利用凿孔把字母信息编码在卡片上的一种方式，后称“霍尔瑞斯代码”。此代码在日后的数据统计工作和 1890 年美国人口普查中发挥了重要作用。霍尔瑞斯还发明了电子触头用以读取卡片信息，系统“读取”数据时，如遇凿孔处，电路将会关闭，如此可将凿孔位置和

数量逐一记录。霍尔瑞斯于1896年成立制表机公司（Tabulating Machine Company），后经上百年的发展，成为了今天的IT“蓝色巨人”——IBM。20世纪80年代以前，该凿孔式卡片信息输入方式在世界范围内被广泛应用。

20世纪40年代，一种利用增减计数轮读取和记录数字信息的机器被发明出来，人们称之为“会计计算机”。这种能电子“读取”和记录数据的机器为日后现代计算机的发明奠定了良好的基础，那些老旧的对数或其他函数制表以及进行加减乘除计算的手动机器必将被取代。

1944年，人类发明了首台电子计算机ENIAC 1，标志着信息时代的到来。小托马斯·J. 沃森（Thomas J. Watson Jr）曾在1943年公开发表了一段著名的声明，即“我认为在不久的将来，或许全世界将需要5台电子计算机。”IBM的档案显示：公司总裁小托马斯·J. 沃森先生在1953年发表的一份股东告知书中曾这样写道，“新一代IBM701电子数据处理器将解决人类20个最关心的问题。”

果不其然，在其后的半个多世纪里，我们亲眼见证了计算机给商业带来的巨大改变。人类一下子从“纸笔时代”进入到了由机器核算，计算机、有线网络和无线网络组成的“信息时代”。为了使审计更有效率，会计人员都开始热衷学习计算机知识。比如：学习如何利用流程图对计算机应用程序和控制进行评估及归档；学习如何使用赫斯金斯·赛尔斯审计系统（Haskins & Sells Auditape System）直接访问客户端计算机文件。

20世纪60年代，审计人员只有通过内部审计师协会（The Institute of Internal Auditors）和当时新成立的EDP审计师协会（EDP Auditors Association，现在名为“信息系统审计与控制协会”）来获得有关信息技术审计方面的资讯。那时协会只有为数不多的一些资料，3本具有权威IT审计认证的书籍是：1961年出版的《电子数据处理与审计》（*Electronic Data Processing and Auditing*），作者菲利克斯·考夫曼博士，注册会计师（Felix Kaufman, Ph. D., CPA）；1965年出版的《计算机审计》（*Auditing with the Computer*），作者韦恩·S. 布特尔博士，注册会计师（Wayne S. Boutell, Ph. D., CPA）；1968年出版的《审计与电子数据处理》（*Auditing and*