安全技术经典译丛

CISA
认证学习指南（第4版）
注册信息系统审计师

CISA: Certified Information Systems Auditor
Study Guide, Fourth Edition

[美] David L. Cannon 著
Brian T. O'Hara 参编
Allen Keele
白大龙 译

100%涵盖CISA最新学习目标，全面讲解IT治理、IS审计流程、系统实施和运行以及保护信息资产等主题

SYBEX
WILEY
清华大学出版社

安全技术经典译丛

CISA 认证学习指南(第 4 版)

注册信息系统审计师

[美] David L.Cannon 著
Brian T. O'Hara
Allen Keele 参编
白大龙 译

清华大学出版社
北 京

David L.Cannon, Brian T. O'Hara, Allen Keele
CISA: Certified Information Systems Auditor Study Guide, Fourth Edition
ISBN：978-1-119-05624-9

图书在版编目(CIP)数据

CISA 认证学习指南(第 4 版)　注册信息系统审计师/ (美) D.L.坎农(David L. Cannon)著；白大龙 译. —北京：清华大学出版社，2017
(安全技术经典译丛)
书名原文：CISA: Certified Information Systems Auditor Study Guide, Fourth Edition
ISBN　978-7-302-47809-6

Ⅰ. ①C… Ⅱ. ①D… ②白… Ⅲ. ①审计－资格考试－自学参考资料 Ⅳ. ①F239

中国版本图书馆 CIP 数据核字(2017)第 170436 号

责任编辑：王　军　韩宏志
装帧设计：牛静敏
责任校对：成凤进
责任印制：李红英

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：35　　字　　数：809 千字
版　　次：2017 年 10 月第 1 版　　印　　次：2017 年 10 月第 1 次印刷
印　　数：1～3000
定　　价：98.00 元

产品编号：072584-01

译 者 序

作为一个新兴领域，信息系统(IS)审计在审计行业和 IT 行业的地位举足轻重。企业很难区分一项工作是由业务部门还是 IT 部门完成的，监管机构或股东们则更想通过 IS 审计来了解业务的真实状况。IS 审计不仅能满足上述两项要求，还能积极推进 IT 水平的提高。

初出茅庐的新手可能觉得 IS 审计十分神秘；IS 审计方面的教材稀缺，从业人员较少，能透彻阐述 IS 审计知识的人更是凤毛麟角。

IS 审计师往往从股东或监管机构的视角审视信息系统；IS 审计是一个高尚的职业，是一项有趣的工作。要成为一名合格的 IS 审计师，需要学习的内容繁多，也需要灵活地综合运用这些知识。

本书是 IS 审计行业的经典书籍，全面系统地从信息系统角度清晰讲解什么是 IS 审计；将引领你步入 IS 审计的神圣殿堂，并顺利通过考试。本书与时俱进更新内容，现已升级到第 4 版，以更紧密地贴合当今的 IT 发展趋势。

本书采用自上而下的编排方式，从管理层的视角入手，剥茧抽丝，基于项目讲解如何开展 IS 审计工作，全面展示 IS 审计视图。开篇概述 IS 审计，此后循序渐进地讲解 IT 治理、IS 审计程序、网络技术基础、IS 生命周期、系统实施、系统运行、信息资产保护以及当前最热门的业务连续性相关知识。

为帮助学员更轻松地通过考试，每章末尾都附加一些习题。这些习题非常接近于考试题目，对你深入理解本书的概念很有帮助。

本书由白大龙翻译，参与翻译的还有赵利通、王文娟、刘帮生、王岩、孙丽红、丁强、刘玲、郭佳、李麦瑞、卢江江、徐梦迪等。这些人员为本书的翻译投入巨大热情并付出很多心血，非常感谢他们的支持。还要感谢清华大学出版社的编辑们以及排版人员、美工师、封面设计人员，没有你们的辛勤付出，本书不可能顺利付梓。在此一并表示感谢！

对于本书，译者本着严谨认真的态度，在翻译过程中力求准确流畅，但鉴于译者水平有限，失误在所难免，如有任何意见和建议，请不吝指正。感激不尽！

最后祝广大学员顺利通过考试，在 IS 审计行业大显身手，做出一番事业。

译者简介

白大龙 玛泽国际合伙人、玛泽全球预备领导人、中审众环会计师事务所合伙人，中国通信协会信息安全专家，CISA、CISSP、CRMA、CRISC、PMP、ITIL、Cobit、ISO27001LA等认证专家，曾在IBM、Symantec以及在港上市工作多年，主要服务过的客户包括中国人民银行、中国农业发展银行、中国建设银行、中国工商银行、中国移动、中国联通等。自2002年以来，一直从事信息安全、IT审计与咨询研究与实践工作。曾翻译《透视ITIL 3.0三大热点》、《中航工业集团公司500强财务报告》(2013至2016年)、《NATIXIS STRUCTURED ISSUANCE S.A. 2016年度财务报告》等资料。

作者简介

David L. Cannon CISA、CCSP，是 CertTest 培训中心的创始人，CISA 培训的领军人物。David 在 IT 运营、安全、系统管理和企业管理方面有 20 多年的 IT 培训和咨询经验。他为美国各地提供 CISA 备考课程。在信息系统审计领域，他备受尊崇。经常在重要的安全和审计会议上发表演讲。David 撰写的本书的前几个版本，在 CISA 备考指南市场上销量遥遥领先。

本书贡献者简介

Brian T. O'Hara CISA、CISM、CRISC、CISSP，是 Do it Best 公司的信息安全官(ISO)，拥有超过 20 年的安全和审计服务经验，曾为财富 500 强公司的信息安全官，也曾在 PCI、卫生健康、制造业和金融服务业任职提供审计和安全咨询服务。在进入信息系统审计领域之前，Brian 曾在最大的社区学院担任信息技术课程主任，他帮助开发了第一个 NSA 两年信息安全学术卓越中心。除了为 CISA 学习指导做贡献外，他还担任 Wiley ISC CISSP 和 SSCP 学习指南的技术编辑。他目前担任 ISACA 印第安纳州分会的总裁和 Infragard 联盟的印度尼西亚成员，Infragard 联盟是联邦调查局的公共和私人关系合作伙伴，它们旨在保护国家的关键基础设施。

Allen Keele 是公认的学科型专家、咨询顾问，是专注于企业风险管理(ERM)、信息安全管理、治理/风险/合规(GRC)、业务连续性管理(BCM)、欺诈控制和采购供应的业务系统架构师。Allen 撰写了 6 本图书，已获得超过 25 项专业认证，包括 CISA、CISM、CISSP、ISO 31000 CICRA、ISO 27001 CICA、ISO 27001 主任审核员、ISO 22301 注册业务连续性经理和注册欺诈检察官。Allen 经常在会议、展览会和专业会议上为专业协会(如 ISACA)、内部审计师协会(IIA)、安永会计师事务所等组织发表演讲。

自从 1999 年注册信息安全网站(www.certifiedinfosec.com)成立以来，Allen 已经领导 CIS 在业务战略、策略开发和系统开发、系统部署以及企业风险管理审计、业务连续性管理审计、信息安全管理审计、欺诈控制管理审计、采购和供应链管理审计方面提供了非常有价值的培训和咨询服务。他的实践经验范围包括：

- 领导客户的跨职能委员会，为 ERM、GRC、BCM、信息安全和欺诈控制制定符合标准的程序架构和战略，以支持组织目标，并满足行业具体的合规要求。
- 帮助客户建立必要的战略、管理领导力、政策和协议，以支持组织获得 ISO 22301 业务连续性管理、ISO 27001 信息安全管理、ISO 9001:2015 质量管理体系和 ISO 14001:2015 环境管理体系的认证。
- 组织关键集团执行开发会议建立跨越企业的专业管理能力。
- 领导程序类项目启动和部署。
- 帮助组织定义操作风险评估和业务影响评估所需的风险背景、标准和范围。
- 帮助组织制定正式的风险评估和风险处置方法。
- 引导风险所有者和审计人员进行操作风险评估、信息安全评估、欺诈风险评估和业务连续性计划评估。

可通过 CIS 总部的电话+1 (904) 406-4311 或邮件 allenkeele@certifiedinfosec.com 联系 Allen。

技术编辑简介

Brady Pamplin，CISSP，在 Control Data Corporation 的多个岗位上工作 28 年，包括程序员、讲师、费用分析师和项目经理。在 CertTest 培训中心任职 2 年期间，Brady 主讲了多场 CISSP 备考课程，并且协助作者翻译了 *CISA Certified Information Systems Auditor Study Guide* 一书的第 1 版，他也是随后该书三个版本的技术编辑。Brady 也曾在电信公司担任系统和网络管理员，在 2011 年，他从阿尔卡特-朗讯公司的网络架构师岗位上退休。

前　言

本书旨在帮助任何对注册信息系统审计师(Certified Information Systems Auditor，CISA)感兴趣且想通过认证的人提供直接的、诚恳的指导。CISA 认证是市场上最热门的入门级审计师证书之一。

在全球范围内，各种组织升级安全级别并证明自己存在强有力的内部控制是一种大趋势。你可能听说过以下几种规定：

- 国际巴塞尔协议 III 银行业风险管理协议。
- COSO，其中包括国家的几个变体。美国版本的萨班斯-奥克斯利法案(Sarbanes-Oxley Act，SOX)针对公共企业提供等同于全球其他证券交易的控制。
- 安全港国际信息隐私保护。
- 美国联邦信息安全管理法案(Federal Information Security Management Act，FISMA)。
- 用于信用卡处理的支付卡行业(Payment Card Industry，PCI)标准。
- 健康保险便携和责任法案(Health Insurance Portability and Accountability Act，HIPAA)。

这些只是 30 多个高级规定中的几个，这些规定都要求提供内部控制的审计证据。坦白而言，他们为 CISA 提供了很多机会。这可能是你一直在寻找的机会，特别是如果你拥有财务或技术背景。

监管合规报告面临的最大问题之一是个人运行测试应用程序，但不了解所有需要完成的其他目标。仅运行软件永远不会让一个人成为合格的审计师。在测试应用程序之外存在太多的依赖项。为了解决这个问题，在心态上，审计师需要保持怀疑态度并加上严格的书面程序、测试计划、失败的实际报告(即使它们是程序性的)，并且要在范围和决策上保持客观独立性，这比只生成单独的测试结果要重要得多。

CISA 认证概述

ISACA 是世界上最公认的信息系统审计资格认证机构之一，提供注册信息系统审计师(CISA)认证。由于优秀的营销推广，它在全球得到了认可。ISACA 的成员遍布 180 多个国家，被公认为 IT 治理理论、控制理论和各种保证准则的提供者之一。ISACA 于 1969 年开始成立电子数据处理审计师协会，目的是制定具体的国际信息系统审计和控制标准。大部分内容是由 Treadway 委员会(Committee of Sponsoring Organizations，COSO)赞助组

织委员会发布的全球财务控制所得出的控制点。因此，ISACA优秀的营销机制建立了知名的信息系统审计师认证——CISA。

ISACA控制全球的CISA考试。它是IT治理和IT咨询中最常见的资格证书之一。与其他ISACA认证一样，CISA很容易获得，因为你不必执行单一审核程序来获得认证。另外你可能遇到的公认的认证证书是由内部审计师协会 (Institute of Internal Auditors，IIA)颁发的注册内部审计师证书(Certified Internal Auditor，CIA)。

CISA的市场前景

CISA仍在不断向全球推广，但技能差距正在迅速扩大。在2008年全球银行倒闭后，企业正在不断招聘和企图留住顾问，努力在因合规性受到处罚之前证明其合规性。咨询公司倾向于联系通过CISA认证的专业人士来为客户提供服务。如果大型和小型组织无法表现出更强的内部控制水平，那么会发现自己处于竞争劣势。一个组织可能因为“太大而不能失败”的神话已被证明是虚假捏造的。我将在第1章中向你举例说明这一点。

审计的基本规则之一是：参与审计中发现问题的修复(修正)会损害审计师的独立性和客观性。审计师必须保持独立性，或至少客观认证结果是有效的。另外，审计师应该协助进行整改工作。监管合规性的要求需要持续保持有效，这意味着在某种程度上的补救措施也将持续保持有效。换句话说，审计师的要求实际上增加了一倍。客户需求也在大幅增加。

100多年来，组织不断地开展财务审计。随着金融系统变得越来越复杂，计算机自动化引起了人们对电子财务记录完整性的担忧。过去，一个组织只会聘请一名注册会计师审查其财务记录，并证明其诚信。更大型的组织则聘请经过认证的内部审计师，协助审查业务的内部控制，帮助减少外部审计的持续成本。现在，内部控制的需求一直集中在信息系统上。计算机现在是财务记录的存储间。只有经过验证、测试，功能齐全的安全控制被证实确实存在，管理人员和员工才可能对电子记录中的篡改或虚假陈述负责。如果你无法证明计算机环境的完整性，也就不能相信电子记录的完整性。

成为一名CISA的理由

大多数未经认证的审计师不仅是善意人士，也是习惯性地违反官方审计标准的人员。下面简要列出了成为一名CISA可以获得的相关优势。

展示专业能力的证明

CISA证书足以证明，你已经掌握了基本的审计理论并且通过了书面认证考试。考试测试了你对与信息系统相关的审计概念和词汇的了解。你的CISA证书已经表明你了解将审计概念应用于信息系统这个抽象世界的基本原理。

可为你的雇主提供增值服务

今天的雇主对认证的价值是非常了解的。你对 CISA 的学习将提供新的方法来提高你的工作绩效。最初，个人通过模仿资深人士来开展类似的审计工作是相当普遍的(俗话说，“猴子看，猴子做”)。目的是突出你应该遵循的做法，即使你以前从未听说过。在你已经奠定基础并更好地了解概念后，你的工作表现将会得到改善。通过 CISA 考试后，你可以进行额外的实践培训，这样才可以独立执行每个审计程序。

是审计团队成员能力的基本证明

CISA 是审计团队中履行审计职能的成员的最低能力证明。审计客户的要求是非常苛刻的。客户组织的命运可能取决于审计师报告中的详细结果。几乎没有可以犯错的余地。CISA 证书可以表明，你了解足够的理论，了解如何提供值得信赖的审计结果。一些被审计的企业会试图误导你对应该报告的内容不进行报告。阅读审计报告的人需要确定你的工作是准确无误的。客户将根据你提供的报告指导资金和资源的消耗。CISA 认证有助于证明你不是偏爱技术的人员伪装成的审计师。

可增加你的市场价值

CISA 证书被视为入门级专业技术审计师的起点。没有比这更好的办法吸引管理层的重视。你是否在组织内部或外部无关紧要。具有更多侵入性要求的政府法规正在成为高级管理人员日益关注的问题。客户可能不了解审计师工作的所有细节；但是，你的客户会认识到即使你可能不知道实际的审核程序，你可以聪慧地谈论目标。此外，审计公司可以为认证专业人员提供更多的资金。

提供更大的晋升机会

每个组织都为有自我激励的优秀人才提供机会。别人对缺乏认证的人怎么看？他们是没有动力？没有能力？还是只是害怕尝试？没有任何经理会在心中正确看待一个没有证书证明其价值的人。花时间去接受教育，向世界展示你有能力。获得证书证明你是有能力完成工作的人。你的 CISA 证书不需要你用语言来描述你的能力，而是直接表明你对自己的工作很认真，人们会相应地对待你。

建立学习审计程序的信心

今天的世界要求非常专业。想一想是不是今天世界上许多优质价值的产品都经过了认证。我们已经认证了二手车、认证了邮件、认证了会计师、认证了焊工、认证了导游、认证了律师，甚至认证了三明治艺术家。坦白而言，贸易行业比 CISA 在教学实践程序和技术方面的表现要好 20 多倍。要成为发型师或食品服务经理则要困难得多，因为这些需要数月的全面性的训练才能完成所有的学习任务，才能通过认证。幸运的是，CISA 培训只回答了“为什么”这一理论性的问题；你去其他地方进行培训，是学习“如何”执行具体的审计。CISA 是你渴望成为受人尊重的白领的第一步。

本书读者对象

如果你真想成为一名专业的信息技术审计师，那么本书正是你所需的。如果你对成为 CISA 审计师或降低合规成本感到好奇，那么在本书中你将学会如何操作才能成为一名优秀的审计师。

进入技术审计领域的人员通常有以下特征之一：

- 金融专业人士寻求更有趣的不断向上的挑战。
- 工业控制专业人士渴望提高他们的理解以获得认可和提高。
- IT 专业人士希望离职运维工作，拓展到有利可图的咨询或渗透性测试行业。
- 内部审计师试图揭开 IT 内部的控制问题(从新闻报道来看，我们都知道太多审计师没有正确地测试控制元素)。

本书在信息系统审计领域是独一无二的。你可以从中学习成为一名成功的审计师需要的所有工作流程和决策点。这些章节让你逐步实现你的目标。本书讲述如何完成工作、通过考试目标(每章开头列出)以及掌握所有最重要的审计概念。

为什么本书是你的最佳选择

本书旨在帮助你成为受人尊敬的 CISA。在这里没有混乱的概念或填鸭式的练习。CertTest 已经多次成功举办 CISA 研讨会，并拥有多年的杰出培训经验和优良的成绩。本书永远不会取代现在的“See-Do-Run”研讨会，教你了解如何执行程序，但这将有助于你通过 CISA 考试。考试只是你职业生涯中的一块垫脚石。通过考试并不能证明你就是一名出色审计师。它只是给你的客户一个再听 15 秒钟的理由。现在你有 15 秒钟来证明你知道自己在说什么。

想象一下，告诉某人你是一个经过认证的火焰剑的玩家。你可以打赌，他们的下一个评论肯定是，“真棒。点燃剑，开始玩吧。”当你通过执行任务向他们展示你的技能而不只是通过考试来证明，会给客户留下深刻的印象。本书的目标是通过向你展示信息系统审计工作中“如何做和为什么这样做”，让你比其他任何人更了解 CISA 的实质。

- 如果你熟悉技术，本书将帮助你了解审计师必须如何行事才能取得成功。IT 专业人士常会成为糟糕的审计师，因为审计是首先了解业务细节。而技术是实现业务目标的次要工具。成功是指通过合法合规来实现企业财务的目标。你只需要关注审计师如何工作，而不必像技术支持人员那样思考。审计师不是技术人员。
- 如果你拥有财务背景，我将带你了解技术。CISA 不是技术人员的考试。本书中的解释在技术上是正确的，目的是使其易于理解。

对于信息系统审计应如何执行有许多不同的观点。本书涵盖了 COSO 法规、ISO 标准与 ISACA 标准的官方审计标准的集合。理解这些标准是你成功的必要条件。放心，它们通常不会相互冲突。如有疑问，应始终优先遵守法规和 ISO 标准。你会发现本书包含

了内部审计或成功的咨询实践所需的宝贵信息。最初的重点是帮助你通过考试。但如果你使用此信息，将发现这些信息可以帮助你获得更多纸质证书。

本书的每一章都按照实际应用的逻辑顺序排列。ISACA 的内容材料由作者委员撰写，每个都有自己的页面。我们选择了不同的路线。本书中的材料是按照 CertTest 在审计之前用于教育自己员工和客户的顺序编写的。

你将首先了解基础知识，并建立你的学习方式，除非有新教材，否则是没有重复的。强烈建议你按顺序阅读章节，不要向前跳过任何章节，因为每章中的材料对于理解后续章节中的材料都很重要。因此，专注于具体章节可能导致顺序混乱，因为每个章节不是独立的知识单元。

如何成为一名 CISA

根据 ISO 的最低认证标准，被证明有能力满足以下五项要求的个人可以通过 CISA 认证。

通过 CISA 考试

CISA 每年提供三次考试机会，6 月、9 月、12 月各一次。你必须提前三个月注册考试。可以在 www.isaca.org 在线注册或通过邮件注册。考试是在现场监视员面前利用铅笔和纸张完成。它包含 200 个选择题，有 4 小时的考试时间。在离考试结束“十分钟左右”时会提醒考试马上要结束，你只可以再做几道考试题。通过 CISA 考试需要 450 分以上的成绩，并且你必须位于 ISACA 评分曲线靠前的三分之一范围。

信息系统审计、控制或安全方面的专业经验

由于 CISA 不检查或测试任何人执行任务的能力，因此你必须拥有五年的信息系统审计经验，才能证明你拥有足够的入门级基本知识，才能成为审计团队的成员。ISACA 可以接受长达两年的替代工作经验要求，具体如下。

- 可替代的相关经验

你的财务、运营审计或信息系统经验替代最多一年的相关经验。

- 大学信用时间替代

你的副学士(大专)或学士学位，可分别替代一年、两年(60 小时或 120 小时)的经验。

- 大学导师体验替代

全职大学教师可用两年的在职经验替代 IS 审计控制或信息安全一年的经验。

你的 CISA 考试成绩自考试日期起有效期为五年。即使没有任何相关的工作经验，也可以参加 CISA 考试，以证明你通过了基本理论的书面要求的考试以适应审计团队。在团队中，你可以获得宝贵的经验。只有在你提供所需工作经验(五年或相当于)后，才会颁发认证。ISACA 将可接受的经验限制在申请日期之前 10 年内发生的经验。

持续遵守 ISACA 职业道德规范

信任和诚信是审计师专业至关重要的素质。你将被要求持续保证遵守 IS 审计师职业

道德规范。

坚持符合完善的 IS 审计标准

审计标准的目的是确保审计质量和一致性。不符合这些标准的审计人员将客户、自己和整个行业置于危险之中。ISACA 提供信息，指导审计师履行其专业职责。审计标准是基于全球应用的公认的专业实践。

参加继续教育，保持审计任务能力经过培训和更新

在你通过书面考试后可以立即开始。你需要通过更多的教育来学习如何执行单独的审核程序任务，学习运行不同的分析软件(如 SCAP)，并执行详细的测试过程和许多其他必需的任务，这些任务不在 CISA 考试的学习材料中。通过运行程序来学习总是比阅读和听课更容易。

审计师的工作是应用每个官方行业标准，同时提供优秀的记录，以便其他人可以独立重现相同的结果。当通过匹配其他审计师的结果来测试验证证据时，可以证明工作做得不错。面对十分详细的书面程序，简陋的记录和贫乏实践以及有限的工作效率表明审计师能力的欠缺。

如何使用本书和网站

本书分为 8 章。每个课程都始于与 CISA 考试直接相关的章节目标列表。

每个章节的末尾都会有一个“考试要点”部分，以突出你在考试中可能遇到的主题。必考内容旨在指导你的学习，而不是提供考试清单。当你进入下一章时，目标是帮助你关注于每一章的更高层次的目标。

每章结尾都有基本的问题回顾和解释。你可以借助它们来衡量自己的理解水平，并决定学习重点。当完成每一章时，应该查看问题并检查你的答案是否正确。如果不正确，请再次阅读相关章节。查找任何不正确的答案，并确定为什么答错了这个问题。可能是因为没有阅读这个问题的相关案例，并且考虑了每个可能的答案。也可能是你不理解该信息。无论是哪种可能，通过第二次阅读该章来改进是很有价值的。

我们已经在本书和相关的网站中包含了几项测试功能。“前言”的末尾处有一个评估测试，可以帮助确定你的学习要求。在开始阅读本书之前先进行这个测试。它将帮助你识别对你的成功来说至关重要的领域。评估测试的答案位于最后一个问题之后。每个答案都包括一个简短说明，这个说明将引导你去查看相关章节以获得更多信息。

本书的在线学习环境网站为 sybextestbanks.wiley.com，其中包含了两套有 200 道问题的练习题。另外还有 300 多张 Flash Card。你应该将本学习指南与其他材料结合使用，以准备考试。

在练习这些考试题目时，应该假设你正在参加考试。只要坐下来，开始做每道练习题，就不要参考任何资料。建议你在本书中结合相关 ISACA IS 审计标准材料进行学习。由于时间限制，正式的 CISA 考试还是非常具有挑战性的。大多数人在时间用完之前可

能没有完成考试题。幸运的是，CertTest 的学生成功率很高。你有权成为下一个通过 CISA 认证的学员。

若在实践考试和章节审查问题中得分高于 90%，则说明你已经达到 CISA 考试要求的水平了，可以参加考试了。

网站上包含了一些考试习题，请你按照实际的 CISA 考试的速度进行计时。

本书主要内容

本书包括许多有用的内容，旨在帮助你准备 CISA 考试。

评估测试

在本书前言末尾的评估测试可用于快速评估你对信息系统审计和审计基本概念的了解。在开始学习本书之前，应该先进行这个测试，这样有助于你确定自己的强弱领域。请注意，这些问题比你在考试中遇到的问题要简单。

目标地图和开放目标清单

本书开头给出了详细的考试目标图，显示了本书涵盖的每个考试目标。另外，每章都会以一个考试目标清单开篇。

考试要点

每章以简要概述该章所涵盖的概念为结尾。我建议仔细阅读这些部分，以检查你对每个主题的记忆，并回到该章重新查看你尚未掌握的部分。

每章的问题回顾

每章都包括问题回顾。这些问题的材料直接从该章所提供的信息中筛选而出。这些问题都是以考试为目标，难度与 CISA 的实际考试相当。

互动式在线学习环境与测试库

本书的互动式在线学习环境提供了测试库作为学习工具，帮助你准备认证考试，并提高你首次通过认证考试的概率！测试库包括以下内容。

考试样题

本书中所有的问题都在评估测试习题中提供，你将在本前言的最后看到该评估测试习题，另外，在每章的最后也包含一些问题回顾。此外，还有两套练习题。通过这些问题可以测试你对学习指南中知识的掌握程度。在线测试库可以在多个设备上运行。本版本中新增了一些功能，超过一半的扩展练习考试题来自本书的贡献者 Allen Keele 和他编

写的 *AllenKeele's 2016 CISA SuperReview*。

记忆卡

问题可以以数字记忆卡的格式提供(一个问题后面紧跟一个正确答案)。也可以使用记忆卡加强你的学习，并在考试前热身。

其他学习工具

书中的关键术语词汇表以可搜索的 PDF 格式提供。

访问 http://sybextestbanks.wiley.com，通过注册就可以访问互动式的在线学习环境和带有学习工具的测试库。一旦注册，也可以参与限时促销活动，只有购买 *AllenKeele's 2016 CISA SuperReview* 一书时才可享受折扣。

如何使用本书

如果你想为 CISA 考试做好准备，那么就别再找其他书籍了。我花了很多时间整理这本书，唯一的目的是帮助你通过考试！

本书涵盖了很多有价值的信息。如果你遵循下列所述的方法，将可以充分利用学习时间：

(1) 阅读完本前言后立即进行评估测试(答案在测试题的后面，但不要偷看！)如果你不知道任何答案也没关系，本书的目的就是让你知道你原来不知道的内容。仔细阅读任何你做错的问题的解释，并记下这些材料所在的章节。

(2) 仔细学习每一章，确保你充分了解每章开头所列的信息和考试目标。再次要特别注意你在评估测试中做错的问题所在的章节。

(3) 回答每章末尾的全部复习题。要特别注意让你产生困惑的任何问题，并再次学习这一章节相应的部分。不要只是走马观花地了解这些问题，请确保你完全理解每个答案。

(4) 使用所有电子记忆卡进行测试。这是一个全新的和更新的记忆卡程序，帮助你准备最新的 CISA 考试，这是一个非常棒的学习工具。

本书中每一份学习材料的理解都离不开你良好的学习习惯。所以尽量在每天相同的时间，选择一个舒适安静的地方来学习。如果你努力学习，就会惊讶于你学习这些材料的速度。如果你按照复习题、练习考试和电子记忆卡的顺序进行学习，将增加你通过考试的概率。

CISA 考试的目的

当然，你可能对考试中遇到的问题类型感到好奇。ISACA 对实际的考试题目保护非

常严格。下面介绍 CISA 考试的设计方式。

- CISA 考试不是 IT 安全测试。要求考生要了解审计的基本概念和术语。然而，IT 安全知识本身并不能帮助考生通过考试。
- CISA 考试不是财务审计师的考试。不要求考生是会计技术员或执行复杂的金融交易的人员。
- CISA 考试不是电脑技术员考试。不要求考生会搭建计算机或配置网络设备。只是希望他们理解常见的术语。
- 整个重点是如何将财务审计的结构化规则应用于管理信息技术的抽象世界。

通过正确学习本书，你可以更好地了解顺利通过 CISA 认证的方式和技巧。只要记住，信息系统审计师是经过特别训练的观察员和调查员。我们不解决实际问题，而是采用结构化调查程序发现问题，之后报告调查结果。了解如何获得正确的证据是关键。

CISA 考试失败的原因

CISA 考试是基于 ISACA 的审计标准和“审计准则声明(Statements on Auditing Standards，SAS)”而设计的。IT 的抽象概念要求审计师使用不同的审计方法。人们可通过直接经验或与其他人交谈来学习。以下是考试失败的两种原因。

同一问题复习超过两次

一个非常不好的坏习惯是用练习题来模拟考试。研究证明，大脑在第二次通过相同的问题后会停止学习，然后开始记住措辞。这使得大脑将答案记录为记忆，而不是学习信息。因此，由于 ISACA 使用不同的风格提出问题和选择答案，你可能会错过正确的考试答案。

另一个大问题是使用互联网提供的无法追溯到官方参考资料来源的练习题。糟糕的问题可以让销售者赚钱却给你提供错误的信息。请注意隐藏在网站后面的幽灵销售商，他们不会向你显示完整的联系信息。我建议你坚持使用本书或 CertTest 网站提供的问题或购买 ISACA 官方练习题。两次通过后不要再复习同一个问题。相反，应该重读本书中的相应部分。

不正确的准备方式

CISA 考试旨在防止填鸭式学习。你会发现考试题目的结构相当复杂。一些答案的选项几乎不符合这个问题。只有选择尊重审计目标的精神和意图的才是最佳选项。有可能最佳的答案只有 51%的正确性。但是如果这是最佳的选择，那么就可以用 51%正确性的答案。这种混乱是有意的，以防止参加考试的人采用死记硬背的方式。最好的学习技巧是每天阅读使用手册 1 小时左右。请务必阅读所有章节——按顺序阅读每一页。以前的 CISA 考生会感到非常混乱，因为他们发现自己认为最有把握的主题，却答得不理想。你可能有很多年的经验，但重要的是你的观点与 ISACA 的考试要保持一致。我没有听说过一个人在抵触正式的考试问题后能得到更好的成绩。ISACA 使用专业测试公司进行考