Mc Graw Hill Education

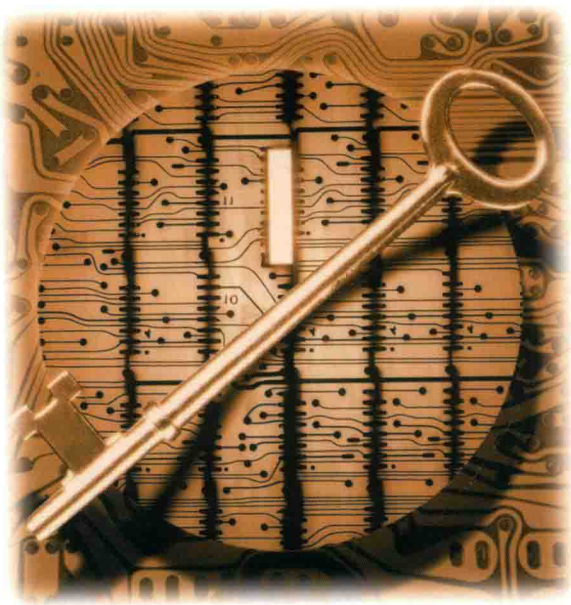
安全技术经典译丛

ALL · IN · ONE

CISSP EXAM GUIDE #1

CISSP

认证考试指南(第7版)



全新覆盖信息系统安全认证的所有8个专业领域

最理想的学习工具和工作参考书

丰富的练习题和深入透彻的解答

配套1400多道练习题

[美] Shon Harris　Fernando Maymí　著　　唐俊飞　译

Mc Graw Hill Education

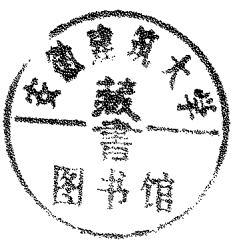
清华大学出版社

安全技术经典译丛

CISSP 认证考试指南

(第 7 版)

[美] Shon Harris
Fernando Maymí 著
唐俊飞 译



清华大学出版社
北 京

Shon Harris , Fernando Maymí
CISSP All-in-One Exam Guide, Seventh Edition
EISBN: 978-7-07-184927-2

图书在版编目(CIP)数据

CISSP认证考试指南(第7版) / (美)肖恩·哈里斯(Shon Harris)，(美)费尔南多·梅密(Fernando Maymi) 著；唐俊飞 译. —北京：清华大学出版社，2018
(安全技术经典译丛)
书名原文：CISSP All-in-One Exam Guide, Seventh Edition
ISBN 978-7-302-49149-1

Ⅰ. ①C… Ⅱ. ①肖… ②费… ③唐… Ⅲ. ①信息系统－安全技术－资格考试－指南 Ⅳ. ①TP309-62

中国版本图书馆 CIP 数据核字(2017)第 311978 号

责任编辑：王 军 韩宏志
装帧设计：孔祥峰
责任校对：成凤进
责任印制：王静怡

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 刷 者：清华大学印刷厂
装 订 者：三河市铭诚印务有限公司
经 销：全国新华书店
开 本：185mm×260mm 印 张：61.25 字 数：1686 千字
版 次：2018 年 1 月第 1 版 印 次：2018 年 1 月第 1 次印刷
印 数：1~4000
定 价：158.00 元

产品编号：071181-01

从业人员对本书的赞誉

Shon Harris 撰写的 CISSP 权威指南为 CISSP 认证提供了极有价值的工具书。Fernando Maymí 用明晰、准确和客观的行文传承了这种优秀精神。

我相信 Shon 会为此深感欣慰和自豪。

David R. Miller

CISSP、GIAC、GISP、PCI QSA、SME、MCT、MCITPro Enterprise Admin、MCSE NT 4.0, 2000, 2003, 2008、CEH、 ECSA、 LPT、 CCNA、CWNA、CNE、GIAC GISF、CompTIA Security+等

一本优秀书籍。内容清晰明了，对学习者、教育工作者和从业者都极有价值。

Joe Adams 博士

Michigan cyber range 创始人兼执行董事

Maymí 和 Harris 撰写的本书通俗易懂，极具启发性，指导你全面了解网络安全。

Greg Conti 博士

Kopidion 有限责任公司创始人

多么希望在职业生涯早期就能阅读到本书！毫无疑问，我仅用这本书就通过了 CISSP 考试，但更重要的是，我从这本书中学到许多以前不了解的、不同方面的安全知识。从这本卓越书籍中汲取的知识将在未来几年一直帮助到我。

Janet Robinson

首席安全官

本书在战略、操作和战术方面呈现保护政府、企业数据中心和网络的知识，将帮助学员有力地阻止网络攻击。

我使用 Shon 的这本书顺利通过了 CISSP 认证，因此向全球读者推荐本书。我曾在多家大企业担任管理职位，在将想获得 CISSP 认证的人送到 CISSP 培训班前，我会要求完成两件事。首先，必须证明他们读过 Shon 的这本书；第二，他们必须参加免费的在线 CISSP 预备会。我通过这种方法取得了巨大成功。

我对未来的版本充满期待。

Bill Ross

CISSP、CISM、IAM、SABSA、ITIL、资深情报官

Shon Harris 和她撰写的本书是我取得成功的秘诀。我在 RSA 工作期间聘请了 Shon，使全球 90% 的销售工程师都获得了 CISSP 认证，这全部得益于本书。后来，我把这个项目带到赛门铁克，Shon 和我继续一起确保赛门铁克的安全工程师和安全主管获得同样的结果。本书讲解明晰，为每个人提

供了考试所需的具体信息。本书还有一个优点，能让目前的安全专业人员扎实掌握大量基础知识。能在职业生涯之初就获得 Shon 和本书的指导，我备感荣幸！

Rick Hanson, CISSP
赛门铁克安全业务部门经理

我毫不犹豫地推荐 Shon Harris 撰写的这本 CISSP 认证考试必备指南，本书将指引读者更广泛深入地了解信息安全世界。

Mike Rabbits
CISSP、CISA、信息安全官

所有想获得 CISSP 认证的人士的必备书籍。

Clement Dupuis, CD
CCCure 系列网站所有者和创始人 www.crrure.org

一本出类拔萃的 CISSP 应试书籍。

Sabyasachi Hazra

CISSP、CISA、CISM、PMP、CCSE、ISO 27001 LA、CEH、CCSP、CCSA、CCSE+、MCSA、CCNP

德勤会计师事务所

我通过本书来学习和备考。乐在其中，回味无穷。
本书的讲解清晰明了，语言幽默，编排合理，这都是成功所需要的。
谢谢你的伟大著作帮助我通过考试，永远感激不尽……

David Broda

Shon Harris 用简单的方式阐释最复杂的技术，令人惊叹！这是用来准备 CISSP 考试的好书，也是任何安全技术人员必备的重要参考手册。

Casey Batz
VMware 网络安全工程师

过去两年，我们区域有 200 多人使用 Shon 的“CISSP 认证考试指南”通过了 CISSP 考试。无论对于初出茅庐的新手，还是拥有一定经验的安全从业人员，本书都是一份伟大的财富。

Alex Number
赛门铁克公司

本书绝对是黄金标准，一站式 CISSP 认证参考！我遇到的所有通过 CISSP 考试 IT 专业人士，都购买了 Shon Harris 这本 CISSP 手册。

C.W Thompson

Shon 在网络安全领域的成就是卓越的，并且擅长将知识传授给他人。单凭这本书的帮助，我就获得了 CISSP 认证。

Tony Bradley
S3KUR3 公司自由撰稿人

Shon 流畅清晰的写作风格方便了阅读和沟通，这是我见过的最佳 CISSP 书籍。

A. Bell

我无法说完这本书有多好！我阅读了本书，参加了考试辅导班，并最终一次性通过考试。

D.A. Smith

我将 Shon Harris 的指南用作主要的 CISSP 考试资料，一次性通过考试。此后我又多次重读本书，从其他来源获取许多习题。总之，我认为这本书足够让你领会所有基础概念，并且比其他资料更容易理解。然而你仍要花时间来学习和准备，因为 CISSP 是一场长达六小时的考试，祝你好运！

D. Wolf

我精通几个安全领域的知识，是经验丰富的资深人员。Shon Harris 的著作读起来令人舒畅，如醍醐，如甘露，最终我读完全书，学会原本感到陌生的一些新知识。参加 CISSP 考试时，我只用三个半小时做完考卷，又用一小时进行检查，最终通过考试。强烈向广大读者推荐本书！

Typeaux

作者简介

Shon Harris，CISSP，是 Shon Harris 安全有限责任公司和逻辑安全有限责任公司的创始人兼首席执行官，她是一名安全顾问，是美国空军信息作战部门的前任工程师，也是一名教师和作家。在2014 年去世前，Shon 拥有并运营自己的培训和咨询公司 13 年。她为财富 100 强公司和政府机构广泛的安全问题提供咨询服务。她撰写了 3 本最畅销的 CISSP 图书，也曾参与撰写 *Gray Hat Hacking: The Ethical Hacker's Handbook* 和 *Security Information and Event Management(SIEM) Implementation*，并担任 Information Security Magazine 的技术编辑。

Fernando Maymí，**博士**，CISSP，拥有逾 25 年的安全领域工作经验。他目前领导一个多学科小组，负责网络空间操作的颠覆性创新，并试图通过加强公共部门与私企的合作关系来更好地保护网络空间。Fernando 曾在美国和其他国家担任政府和私营部门组织的顾问。在美国和拉丁美洲，他为学术、政府和专业机构讲授了数十门网络安全课程。Fernando 曾发表十几篇技术文章，并拥有三项专利。Fernando 曾荣获美国陆军研究与发展成就奖，被评为 HENAAC 杰出人物。他与 Shon Harris 密切合作，并为包括《CISSP 认证考试指南(第 6 版)》在内的诸多项目提供建议。Fernando 还是一名志愿者，致力于盲人导盲，养着两只导盲犬：Trinket 和 Virgo。

贡献者简介

Bobby E. Rogers 是一名信息安全工程师，为国防相关部门提供服务，协助他们加固、验证和认可信息系统。他的职责包括信息系统安全工程、风险管理、认证和认可工作。退休前他曾在美国空军工作 21 年，担任网络安全工程师和导师，并为全球网络提供安全保障。Bobby 拥有信息保障硕士学位，并在马里兰州 Capitol 科技大学攻读网络安全博士学位。他拥有许多证书，包括 CISSP-ISSEP、CEH、MCSE:安全、 CompTIA A+、Network+、Security+和 Mobility+。

技术编辑简介

Jonathan Ham，CISSP、GSEC、GCIA、GCIH，是一名独立顾问，专注于研究大型企业的安全问题，包括策略和程序、人员配备和培训、可扩展的预防、检测和响应技术等。Jonathan 对 ROI 和 TCO 有敏锐的理解，在这方面拥有 12 年以上的经验，他帮助客户实现更大成就，并为公共和私营部门、财富 500 企业提供建议。Jonathan 曾受托培训 NCIS 调查员使用 Snort 对来自地下 2000 英尺的系统网络包进行分析，并被授权对美国最大的一家非军事联邦机构进行培训。Jonathan 是 GIAC 顾问委员会的成员之一，也是 SAN 的讲师之一，负责讲授 SAN 的 MGT414: SANS Training Program for CISSP Certification 课程。他曾参与撰写 *Network Forensics: Tracking Hackers Through Cyberspace*。

作者自序

《CISSP 认证考试指南(第 7 版)》的封面首次印上了两位作者的姓名，这是 15 年来的第一次；开创性著作的新版问世了，而 Shon Harris 却离开了我们。尽管如此，她的思想仍留存在已销售的几十万本书籍中，这些书籍丰富了全球安全专业人员的生活。毫不夸张地说：Shon 是安全领域最有影响力的作家之一。她的遗产存在于这个最新版本的每一页上。

这个最新版本的目标是匹配新修订的 CISSP 知识体系，并让你在阅读每页文字时听到 Shon 的声音。本书的大部分内容实际上是 Shon 撰写的。虽然我们已经重新组织、提高、润色和更新了本书，但大部分文字仍出自她手。如果你已经阅读过 Shon 的其他作品，或有幸遇到过她，你将在这些文字中识别出她的风格。我们也希望你能在专业发展的各个方面感受到她对“卓越”的追求。

本书的目标不仅是帮助你通过 CISSP 考试，而且要为你提供基础知识；无论你是否通过认证考试，这些知识都能让你成为专业的信息安全人员。如果你在职业发展中力求卓越，获得 CISSP 认证将水到渠成。你需要将时间和精力投入到可能似乎没有直接回报的主题和问题上。这样做是没什么问题的，每个人都有自己的强项和弱项，但许多人倾向于加强前者而忽视后者。这会导致一个人在非常具体的主题中有足够的深度，但在新的和意想不到的条件下，由于缺乏更广泛的知识而无法更好地成长。我们提出这些，目的是逆转这种本能趋势，我们要在弱点区域付出更多努力。我们的观点是：要平衡成为专家的欲望和全面发展专业的需要。这是组织和社会对我们的要求。

“专业人士”的定义可描述为一群值得信任且训练有素的人，他们提供社会上其他领域的人士无法独自完成的关键服务。CISSP 专业人员要确保信息系统的机密性、完整性和可用性。这些都不能简单地被最优秀的防火墙管理员、取证人员或逆向工程师所执行。我们需要掌握广泛的知识，这样才能为该工作选择合适的工具。要掌握这些相关知识，我们需要学习看似不相关的基础知识。因此，要成为有能力的专业人士，我们都需要专注于学习这些不会立即发挥作用的主题。

本书是一本百科全书，它呈现可直接应用的知识和基础知识。它一直是一本学习指南和参考资料。我们希望：在你获得 CISSP 认证后，你可以一次次地了解你的弱势领域，并指导自己终身自我学习，追求卓越成就。

序　言

非常荣幸能向全球网络安全专家介绍《CISSP 认证考试指南(第 7 版)》一书。这本学习指南对于追求 CISSP 认证的人员而言是至关重要的，应该是每位网络安全专业人士收藏的经典图书之一。

历经 39 年的陆军职业生涯，我很清楚成为职业人员的意义，以及共同价值观、共同语言和身份的重要性。通过培训、教育和经验获得专业知识是通往职业化道路的关键因素，而获得具有明确标准的正式认证是成为网络安全专业人员的最佳选择。

在执行每项任务时，我都寻求充分利用技术和提高数字化水平，并确保我们的运营领域没有风险。今天的威胁加上我们的脆弱性和潜在后果，造成了新的运营现实：国家面临安全风险。当我们进入任何网络时，必须努力确保安全；作为专业人员，网络安全专家需要思考和战胜网络空间的威胁。

随着世界相互连接变得更加紧密，可以预测，网络威胁将继续呈指数级增长。技术网络工作者必须设法阻止威胁和减少漏洞，但我们无法完全消除它们。这就需要专业人士了解风险管理和安全——他们受到信任，致力于创建和提供广泛的安全措施，以降低企业风险，并完成使命，保护所有公共设施和私人财产。

当前，相关领域的专业知识是很关键的，而《CISSP 认证考试指南(第 7 版)》是皇冠上的明珠。在这个最新版本中，Fernando Maymí 保留了 Shon 撰写的优质内容，同时在上一版的基础上进行了拓展。如果正确地使用和学习这本书，你将在个人和专业方面取得长足进步。要获得像专业人士一样值得信赖的能力，本书对你、你的组织都至关重要。

——Rhett Hernandez

美国陆军前指挥官，前中将，美国西点网络现任主席

致　谢

感谢信息安全领域所有富有激情和奉献精神的行业开拓者。信息安全行业的精英就是那些追求道德成果的人。

也要感谢下列人士在我们撰写第 7 版时给予的帮助：

- Ronald Dodge，将这本书的两位作者带到一起。
- David Miller，你的工作热情、忠诚和友谊一直鼓励着我们。
- 所有来自 Logical Security 的同事
- Kathy Conlon，相比其他任何人，为本书第 7 版提供了更多条件。
- David Harris
- Emma Fernandez

最特别的是，我们要感谢你，我们的读者，因为你工作在数字冲突前线，并在你的职业生涯中付出无数努力让我们所有人都能安全地使用网络空间。

纪念Shon Harris

2014年夏，Shon邀我为新版《CISSP认证考试指南》作序。我备感荣幸，下面是原序言的两段。此后我会更多地谈谈我的朋友——已故的Shon Harris。

网络安全仍是一个崭新行业。随着技术的进步，网络安全领域也在不断发展。似乎每十年左右，我们要对发展策略进行一两次更新。20世纪90年代，我们主要关注“边界防御”；许多资金都用在防火墙等边界设备上，以防坏人进入。到21世纪初，我们认识到只有边界防御是不够的，于是“深度防御”方法流行开来，因此我们又花了十年时间，试图建立层次化防御，以发现那些能突破边界防御的坏家伙；为此花费了大量资金，采用的是入侵检测、入侵防御和终端解决方案。之后，到2010年左右，特别是在美国政府发出倡议后，我们开始关注“连续监测”，目标是如果网络中的坏人突破了边界防御和深度防御，还能抓住他们。安全信息和事件管理(SIEM)技术已成为满足这种连续监测需求的最佳解决方案。最近的热门话题是“主动防御”，它指通过动态和变化的防御进行实时响应，这种能力不仅防御攻击者，还包括让组织快速恢复并正常营业。我们开始看到蜜罐与沙盒技术的再次出现，诱惑和捕捉攻击者并进一步分析其活动。在这个简短的历史回顾中，有一个规律是不变的：坏人一直试图进入，即使我们不能在第一时间阻止，也要不断地响应和跟进。这种猫和老鼠的游戏在将来仍会持续，这是可以预见的。

随着网络安全领域的不断发展，为适应新威胁，每个新战略和战术都要求安全专家掌握一套新术语和概念。这样知识体系将变得十分庞大，令人不知所措，特别是对于那些刚入行的新手。我是一名安全从业者、顾问和商业领袖，经常有抱负远大的安全从业者问我如何进入这个领域，我总是建议他们阅读Shon的《CISSP认证考试指南》一书，目的并非让他们一定成为CISSP，而是让他们通过这本书掌握该领域的知识。也经常有经验丰富的安全从业者问我如何在安全领域发展，我鼓励他们获得CISSP认证，并再次让他们参阅Shon的书。一些人最终成为安全领域的领导者，对这些经理来说，CISSP证书是有力的证明。还有其他安全专业人员只是为了寻求更广泛的知识，我也向他们推荐Shon的书，作为一个很好的全面参考书籍。本书经受住时间的考验，不变演进，随着网络安全领域的发展，成为该领域最重要的一本书籍。在我的职业生涯中，已多次提及这本书，并在我随身携带的Kindle中保存着一份副本。简单地说，如果你在网络安全领域工作，也需要这本书。

我几乎不知道，在撰写上述序言的几个月后，Shon将离开我们。我把Shon视为挚友，赞赏她在该领域的贡献。我是在2002年的CISSP集训营认识Shon的。那时我刚开始学CISSP，并在几周内都在上她的课。我当时不知道她已出版过好几本书，也不知道她是该领域真正的领袖。我曾与她在吃午饭时攀谈，在课程结束后的几个月，她联系我：“我记得你对写作非常感兴趣。新项目需要帮助。”在尴尬的停顿后，我回过神告诉她，我觉得自己不够格，但愿意！我多次感谢上帝让我开启了那段经历。那本书就是《灰帽黑客》，现在已是第4版了；此后我得到许多咨询、写作和讲课机会。2008年，我从海军陆战队退休，Shon联系我说：“嘿，有一个为一家大公司服务的机会。你想帮忙吗？”就这样，我有了第一个大客户，创建了我的公司。在Shon的帮助下，这家公司不断成长，在几年后售出。在我认识Shon的12年时间里，Shon一直给予我比想象中更多的机会。她从未要求任何回报，只是说：“你带着它继续吧，我忙着做其他事情。”正如我在海军陆战队服役期间所想的

那样，我把我的大部分成就归功于 Shon。我和他人分享过这个故事，发现自己并不是唯一的；Shon 用她的奉献精神，在安全领域帮助过很多人，谢谢你，Miss CISSP。

Shon 是一个善良、宽厚和谦和的人。如果你认识 Shon，相信你必定有同样的感受。如果你不认识 Shon，我希望通过这几段话，明白她为什么很特别，为什么本书必须会有另外的版本。去年曾有人多次问我："你认为会有另一个版本吗？安全领域和 CISSP 认证都发生了很大变化，我们需要另一个版本。"今天，我很高兴这个新版本问世了。远在天堂的 Shon 必定希望本书能帮助其他人做得更好。我相信，我们作为专业人士，需要将这本书继续下去。我非常感谢 McGraw-Hill 和 Fernando 的团队以这种方式向 Shon 表达敬意，并继续她的事业；这是 Shon 应得的。Shon，你被许多人思念和热爱。通过这本书，你的奉献精神将永存，并帮助更多人。

——Allen Harper，CISSP(感谢 Shon)
Tangible Security 公司执行副总裁

前　言

随着世界不断改变，人们对增强安全、改进技术的需求愈加迫切。每个组织、政府机构、企业和军事单位都开始关注安全问题。几乎所有公司和组织机构都在积极寻求才华横溢、经验丰富的安全专业人员，因为只有这些专家才能保护公司赖以生存和保持竞争力的宝贵资源。而 CISSP 认证能证明你已经成为一名拥有一定知识和经验的安全专业人员。当然，这些知识和经验是认证体系预先规定的，并得到了整个安全行业的理解和认可。通过持续地持有证书，就表明你保持与安全行业同步发展。

下面列出一些获取 CISSP 认证资格的理由：

- 充实现有的关于安全概念和实际应用的知识。
- 展示了你是一位拥有专业知识并且经验丰富的安全专家。
- 让自己在这个竞争激烈的劳动力市场中占据优势。
- 增加收入，并能得到更多工作机会。
- 为你现在的工作带来更好的安全专业知识。
- 表明对安全规则的贡献。

CISSP 认证能帮助公司确认某人是否具有相应的技术能力、知识和经验，从而能从事具体的安全工作，执行风险分析，谋划必要的对策，并可帮助整个组织机构保护其设施、网络、系统和信息。CISSP 认证还能担保通过认证的人员具备安全行业所需的熟练程度、专业技能和知识水平。安全对于成功企业的重要性在未来只可能不断增加，从而导致对技术熟练的安全专业人员的更大需求。CISSP 认证表明，可由被公众认可的第三方机构负责确定个人在技术和理论方面的安全专业知识，并将其与缺乏这种专业知识的普通人员区分开来。

对于优秀的网络管理员、编程人员或工程师来说，理解和实现安全应用是一项至关重要的内容。在大量并非针对安全专业人员的职位描述中，往往仍要求应聘人员正确理解安全概念及其实现方式。虽然许多组织机构由于职位和预算的限制而无法聘请单独的网络和安全人员，但都相信安全对于组织机构自身来说至关重要。因此，这些组织机构总是尝试将安全知识和其他技术知识合并在一个角色内。在这个问题上，如果具有 CISSP 资格，那么你就会比其他应聘人员更有优势。

CISSP 考试

因为 CISSP 考试涵盖了构成公共知识体系的 8 个领域，所以常被描述为“寸之深、亩之阔”。这意味着，考试中出现的问题实质上不一定非常详细，并不要求你在所有主题上都是专家。但是，这些问题却要求你熟悉许多不同的安全主题。

CISSP 考试由 250 道选择题构成，并要求在 6 小时内完成。创新型问题包括拖曳(例如：取一个选项或项目，并将其拖到框中的正确位置)或热点(例如：点击能正确回答问题的项目或选项)界面，但权重和得分与其他任何问题一样。这些题目均来自一个庞大的试题库，从而能尽量做到考题因人而异。此外，为更准确地反映最新的安全趋势，试题库会不断变化和更新，考题则根据需要在库中

经常循环和替换。考试中计入成绩的只有 225 道题，其余 25 道题仅供出题人员研究之用。但这 25 道题与计分的题目毫无区别，因此应试人员并不知道哪些题目是计入总分的。通过 CISSP 考试的最低分数是 700 分(总分是 1000 分)，每道题都会根据难度设定权重，而且并非每道题的分值都是一样的。此项考试不面向特定的产品或供应商，这意味着没有任何问题会针对特定的产品或供应商(例如 Windows、UNIX 或 Cisco)，而是涉及测试这些系统所用的安全模型和方法。

考试提示：

猜测不倒扣分。如果不能在合理时间内找出正确答案，那么你可以猜一个并继续下一个问题。

$(ISC)^2$ (International Information Systems Security Certification Consortium，国际信息系统安全认证协会)还在 CISSP 考试中增加了基于场景的问题。每个问题都向应试者展示一个简短的场景，而不是要求他们区分术语和/或概念。增加基于场景的问题，其目的是确保应试人员不仅知道和理解 CBK 中的概念，而且能将这些知识应用到现实生活场景中。这种做法更为实用，其原因在于现实生活中不可能有人询问你："共谋(collusion)的定义是什么？"此时，除了需要知道"共谋"的定义外，还需要知道如何检测并阻止共谋的发生。

通过考试后，你会被要求提供由担保人认可的证明文件，以证明你确实具有相关类型的工作经验。担保人必须签署一份文件，从而为你提交的安全工作经验提供担保。因此，在注册并支付考试费用之前，一定要与担保人取得联系。你肯定不愿意看到这样的局面：在支付费用并通过考试后，却发现无法找到担保人帮助你完成获得认证所需的最后步骤。

之所以要求提供担保，是为了确保获得认证的应试人员拥有为公司服务的实际工作经验。虽然书本知识对于理解理论、概念、标准和规章极其重要，但绝对不能替代亲身经历。因此，请你一定要证明拥有支持认证实用性的实践经验。

$(ISC)^2$ 将从通过考试的考生中随机挑选少数应试人员进行审查。在审查过程中，$(ISC)^2$ 工作人员将向考生选定的担保人和联系人核实应试人员相关工作经验的真实性。

这项考试的挑战性在于：虽然大多数认证考生都从事安全领域内的工作，但不一定通晓 CBK 包含的全部 8 个领域。虽然某人被视为脆弱性测试或应用程序安全方面的专家，但她可能不擅长于物理安全、密码学或取证。因此，为这项考试而学习将极大地拓宽你在安全领域的知识。

考题涉及构成 CBK 的 8 个安全领域，如下表所示。

安全领域	描述
安全和风险管理	这个领域涵盖了信息系统安全的基本概念。该领域的部分主题包括： • 可用性、完整性和机密性的原则 • 安全治理和合规 • 法律和法规问题 • 职业道德 • 个人安全策略 • 风险管理 • 威胁模型

(续表)

安全领域	描述
资产安全	这个领域解释了在整个信息资产生命周期中如何对信息资产进行保护。该领域的部分主题包括： • 信息分类 • 保持的所有权 • 隐私 • 保留 • 数据安全控制 • 需求处理
安全工程	这个领域解释了在面对无数威胁的情况下如何保护信息系统发展的安全。该领域的部分主题包括： • 安全设计原则 • 选择有效的措施 • 缓解脆弱性 • 密码学 • 站点和设施的安全设计 • 物理安全
通信与网络安全	这个领域解释如何理解保护网络架构、通信技术和网络协议的安全目标。该领域的部分主题包括：安全的网络架构 • 网络组件 • 安全的通信信道 • 网络层攻击
身份与访问管理	身份与访问管理是信息安全中最重要的主题之一。这个领域涵盖了用户和系统之间、系统和其他系统之间的相互关系。该领域的部分主题包括： • 控制物理和逻辑访问 • 身份标识与认证 • 身份即服务 • 第三方身份服务 • 授权方法 • 访问控制攻击
安全评估与测试	这个领域解释了验证我们的信息系统安全的方法。该领域的部分主题包括： • 评估和测试策略 • 测试安全控制 • 收集安全过程数据 • 分析和报告结果 • 开展和促进审计

(续表)

安全领域	描述
安全运营	这个领域涵盖了在我们日常业务中许多维护网络安全的活动。该领域的部分主题包括： • 支持调查 • 日志和监控 • 安全资源配置 • 事故管理 • 预防措施 • 变更管理 • 业务连续性 • 物理安全管理
软件开发安全	这个领域解释了应用安全原则去获取和开发软件系统。该领域的部分主题包括： • 软件开发生命周期中的安全 • 开发活动中的安全控制 • 评估软件安全 • 评估外部获取软件的安全性

为紧跟安全领域的新技术和新方法，(ISC)^2 每年都要在试题库中加入大量新试题。这些试题都基于最新的技术、运用、方法和标准。例如，1998 年的 CISSP 认证考试没有出现关于无线安全、跨站点脚本攻击或 IPv6 的问题。

本书概要

如果你想成为一名经过(ISC)^2 认证的 CISSP，那么在本书里能找到需要了解的所有内容。本书讲述企业如何制定和实现策略、措施、指导原则和标准及其原因；介绍网络、应用程序和系统的脆弱性，脆弱性的被利用情况以及如何应对这些威胁；解释物理安全、操作安全以及不同系统会采用不同安全机制的原因。此外，本书还回顾美国与国际上用于测试系统安全性的安全准则和评估体系，诠释这些准则的含义及其使用原因。最后，本书还将阐明与计算机系统及其数据相关的各种法律责任问题，例如计算机犯罪、法庭证物以及如何为出庭准备计算机证据。

尽管本书主要是为 CISSP 考试撰写的学习指南，但在你通过认证后，它仍不失为一本不可替代的重要参考用书。

CISSP 应试小贴士

许多人考试时会感觉题目比较绕弯。所以一定要仔细阅读问题和所有备选答案，而不是看了几个单词就断定自己已知道问题的答案。某些答案选项的差别不明显，这就需要你花一些时间耐心地将问题再阅读领会几遍。

有人抱怨CISSP考试略带主观色彩。例如，有这样两个问题。第一个是技术问题，考查的是防止中间人攻击的TLS(Transport Layer Security，传输层安全)所采用的具体机制；第二个问题则询问周长为8英尺的栅栏提供的是低级、中级还是高级的安全防护。你会发现，前一个问题比后一个问题更容易回答。许多问题要求应试人员选择最佳方法，而一些人会认为很难说哪一个是最佳方法，因为这都带有主观色彩。此处给出这样的示例并非是批评$(ISC)^2$和出题人员，而是为了帮助你更好地准备这项考试。本书涵盖了所有的考试范围和需要掌握的内容，同时提供了大量问题和自测试卷。大部分问题的格式都采用了实际试题的形式，使你能更好地准备应对真实的考试。因此，你一定要阅读本书的全部内容，同时特别注意问题及其格式。有时，即使对某个主题十分了解，你也可能答错题。因此，我们需要学会如何应试。

在回答某些问题时，要记住，一些事物比其他东西更有价值。例如，保护人身安全和福利几乎总是高于所有其他方面。与此类似，如果所有其他因素都比较便宜，第二个会赢得大部分时间。专家意见(例如：从律师那里获得的)比那些拥有较少认证的人的意见更有价值。如果一个问题的可选项之一是寻求或获得专家意见，请密切关注这个问题。正确的答案可能是寻求那位专家的意见。

尽量让自己熟悉行业标准，并了解自己工作之外的技术知识和方法。再次强调一下，即使你在某个领域是专家，仍然可能不熟悉考试所涉及的全部领域。

当你在Pearson VUE考试中心参加CISSP考试时，其他认证考试可能会在同一个房间同时进行。如果你看到别人很早离开房间，不要感到匆忙；他们可能是因为参加一个较短的考试。

如何使用本书

本书的作者尽了很大努力才将所有重要信息汇编成书；现在，轮到你尽力从本书中汲取知识了。要从本书受益最大，可采用以下学习方法：

- 认真学习每个章节，真正理解其中介绍的每个概念。许多概念都必须完全理解，如果对一些概念似懂非懂，那么对你来说将是非常不利的。CISSP CBK包含数以千计的不同主题，因此需要花时间掌握这些内容。
- 确认学习和解答所有问题。如果不能正确解答其中的问题，那么需要再次阅读相关的章节。需要记住，真实考试中的某些问题含糊其辞，看上去比较难回答，不要误以为这些问题表述不清楚而忽视了这些含糊其辞的问题。相反，它们的存在具有明确的目的性，对此要特别注意。
- 如果你对某些具体的主题(如防火墙、法律、物理安全或协议功能)不熟悉，那么需要通过其他信息源(书籍和文章等)以达到对这些主题更深入的理解程度，而不是局限于自认为通过CISSP考试所需的范围。
- 阅读本书后，你需要学习所有问题和答案，并进行自测。接着，查看$(ISC)^2$的学习指南，确信对列出的每条内容都十分了解。如果对某些内容还感到困惑，那么请重新复习相关的章节。
- 如果参加过其他资格认证考试(如Cisco、Novell和Microsoft的认证考试)，那么你可能习惯于记忆一些细节和配置参数。但请记住，CISSP考试强调“寸之深、亩之阔”，因此在记忆具体细节之前一定要先掌握每个主题中的各种概念。
- 记住该考试是需要找出最佳答案，所以，对于有些问题应试人员可能会对全部或部分答案持不同意见。记住要在所给的4个答案中找出最合理的那一个。