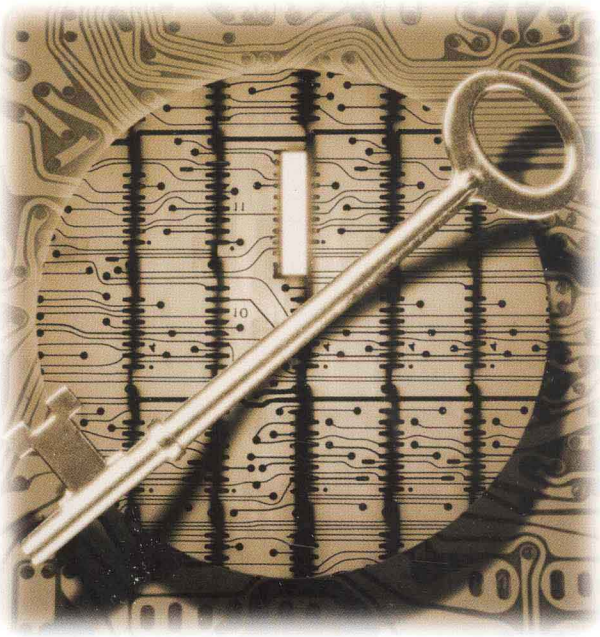
Mc Graw Hill Education

CISSP All-in-One Exam Guide, Sixth Edition

All in One

CISSP EXAM GUIDE #1

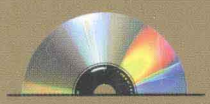
CISSP 认证考试指南（第6版）



最新覆盖信息系统安全认证的所有10个专业领域

最理想的学习工具和工作参考书

丰富的练习试题和深入的解答



电子资料包含了：

- 1400多道练习试题
- Shon Harris的视频培训
- Adobe数字版格式的电子书-免费下载

[美] Shon Harris 著　　张胜生　张博　付业辉　译

Mc Graw Hill Education

清华大学出版社

CISSP 认证考试指南
(第 6 版)

[美] Shon Harris 著

张胜生 张博 付业辉 译

清华大学出版社

北 京

Shon Harris
CISSP All-in-One Exam Guide, Sixth Edition
EISBN: 978-0-07-178174-9

图书在版编目(CIP)数据

CISSP 认证考试指南(第 6 版) / (美) 哈里斯(Harris, S.) 著；张胜生，张博，付业辉 译. —北京：清华大学出版社，2014

书名原文：CISSP All-in-One Exam Guide, Sixth Edition

ISBN 978-7-302-34440-7

Ⅰ. C… Ⅱ. ①哈… ②张… ③张… ④付… 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(2013)第 270024 号

责任编辑：王　军　于　平
装帧设计：牛艳敏
责任校对：邱晓玉
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 刷 者：清华大学印刷厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　印　　张：64.75　　字　　数：1784 千字
（附光盘 1 张）
版　　次：2014 年 1 月第 1 版　　印　　次：2014 年 1 月第1 次印刷
印　　数：1～4000
定　　价：128.00 元

产品编号：051636-01

译 者 序

随着我国信息化技术的蓬勃发展，信息安全问题也越发严重，但信息安全工作还存在很多误区，比如：重技术，轻管理；重解决单个问题，轻规划方案；重计划，轻考核；重 IT 人员，轻业务人员教育；重建设，轻运维保障。这些问题困扰着信息安全从业人员，如何从信息安全原理上分析信息安全各个层面的问题，如何全面地审视信息安全威胁，如何将风险控制到可以接受的程度，《CISSP 认证考试指南(第 6 版)》给出了深入浅出的讲解。同时书中还强调了信息安全要从管理和业务层面入手，设计出信息安全策略，并根据策略进一步落实实施。作者的循序引导将给读者耳目一新的感觉，能够让读者快速建立起自己的信息安全知识体系，不愧是一本经典权威之作。

我从事信息安全工作 13 年，开展大中型企业的信息安全教学工作也已有 8 年，在与数万名学员的交流过程中，我学到了很多知识，我与我的师资团队一起开发了 15 门演练实战课和多门考试认证精讲类课程，在这其中我感受最深的是《CISSP 认证考试指南》中的知识精华给我带来的巨大帮助。

本书全面而细致地讲解了信息安全涵盖的 10 个领域，在每个领域中都贯穿了信息安全风险管理的精髓，作者通过大量案例不断帮助读者拓宽视野，了解行业中的管理和防御实践，本书是参加 CISSP 考试和提高信息安全水平的一本好书！

由于本书知识量大、涵盖面广，在阅读这本书的时候建议大家采用树型图软件梳理，当然关于知识汇总和大家的疑惑交流，也可以访问我的博客 http://blog.sina.com.cn/anquan1000。

本书的翻译过程很艰辛，在此我要特别感谢我的两位搭档：

张博：2005 年开始从事网络与信息安全工作，在一流的网络信息安全公司从事过大量安全项目的实施，并且曾经供职中国移动多年，有深厚的理论知识和丰富的实践经验，在书中的语言描述深入浅出。

付业辉：2002 年起，进入大型跨国企业并一直从事信息安全领域至今，拥有非常丰富的信息安全架构设计和大型安全项目的实施管理经验，对信息安全管理有着国际化的视野。

在翻译过程中，许多人给了我很多帮助，其中包括中国移动集团及各省公司的安全朋友们，向你们积极进取的精神致敬！最后还要感谢我的家人和我的学生们给予的支持和帮助。

本书博大精深，但在实际翻译过程中由于时间和能力所限，肯定存有各种不足之处，恳请读者理解和体谅，也欢迎读者对其中的问题给出批评指正，有关技术问题的交流信箱是 390890513@qq.com。

张胜生
CISSP/CISP/CISA/ISO27001 资深讲师
“红黑演义”云端攻防演练平台总设计师

从业人员对本书的赞誉

我和张胜生老师认识是在教育部 2009 年“第三届中国信息安全学科建设与人才培养研讨会”上，当时张老师在会上做了“大中型企业人才培养”专题发言，那时张老师已经是国内知名的 CISSP 讲师了。《CISSP 认证考试指南》作为行业认可的国际化 CISSP 教材，所涉及的知识领域十分广泛，既适合于行业人士深造所用，同时在高校研究生和本科生教学过程中也可以作为选定教材和参考资料。

朱建明
中央财经大学信息学院院长/教授、博导

IT 和互联网技术已经渗透我们工作和生活的方方面面，互联网金融、手机支付、信息家电、智慧城市、物联网等新兴技术已经逐步由概念变为现实，IT 和互联网技术将与我们的身体健康、财产管理、日常工作、社交活动、 休闲娱乐、个人消费等发生更多更加紧密的联系。因此，IT 和互联网是否安全可靠，将会成为决定我们工作和生活品质的重要因素，网络与信息安全问题已经被提升到了前所未有的高度，而且其重要性还在不断增加。现在很多从业人员、学生和爱好者们都在学习网络与信息安全技术，以实现自己在个人发展、工作需要或者兴趣爱好上的目标。而《CISSP 认证考试指南(第 6 版)》能够满足从业人员、学生和爱好者们的需要，可以在 CISSP 备考时起到极其重要的作用，也可以作为工具书和兴趣读物来使用。

孙晶
首都五一劳动奖章获得者
2010 年北京职工职业技能大赛信息安全比赛冠军

有幸认识张胜生老师是在 7 年前，他那时就已经在 CISSP 教学的第一线奋战多年，CISSP 的理念和知识已经深深融入张老师的血液中。虽然本书是一本国外教材的翻译版，但张老师在翻译本书的过程中，倾注了大量的心血，将自己对 CISSP 教学的丰富经验融入其中，使读者能够更加容易地理解本书原作者要表达的 CISSP 全部内容。

一本好书可以改变一个人的命运和前程，我认为《CISSP 认证考试指南(第 6 版)》就是一本这样的好书。作为 CISSP 认证考试的权威教材，本书以海一样广阔的胸怀容纳了安全行业的方方面面，从不同的角度，不同的主题系统化地阐述了建设和管控企业安全的方法和知识。

如果你是一个安全从业者，我认为这是一本温故而知新，每看一遍都有不一样体会的书。

如果你是一名安全初学者，我认为这是一本指导你走向安全岗位，并获得从业资格的宝典。

聂万泉
阿里巴巴高级安全专家

我是在 5 年前的 CISSP 培训课上认识张胜生老师的，他对信息安全深邃而独到的见解以及丰富的 CISSP 经验，给我留下了深刻的印象。《CISSP 认证考试指南》可以说是 CISSP 考试的宝典，而张老师翻译的《CISSP 认证考试指南(第 6 版)》和他更是相得益彰。

张健
完美世界信息安全总监

作者简介

Shon Harris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，也是教师和作家。自2001年以来，Shon拥有并经营着自己的培训和咨询公司，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，同时还是*Gray Hat Hacking: The Ethical Hacker's Handbook*和*Security Information and Event Management(SIEM) Implementation*的特约作者，*Information Security Magazine*的技术编辑。她还为Pearson出版公司开发了许多数字化安防产品。

技术编辑简介

Polisetty Veera Subrahmanya Kumar拥有CISSP、CISA、PMP、PMI-RMP、MCPM、ITIL认证证书，在信息技术领域拥有20多年的经验。他的专业领域包括信息安全、业务连续性、项目管理和风险管理。他最近担任项目管理协会PMI-RMP(PMI-Risk Management Professional，风险管理专业)资格认证委员会的主席，曾是ISACA印度Growth Task Force团队成员。过去他还曾担任各种PMI标准开发项目的内容开发团队负责人。他还是PMI(美国项目管理协会)PMBOK(项目管理知识体系)培训的首席讲师。

致　谢

我要感谢所有在信息安全领域富有激情、具有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。

我要感谢那么多的圈内人愿意花时间联系我，并让我知道我的工作直接影响着他们的生活。我感激人们花时间和精力反馈给我这些信息。

我也要感谢下列人士，在我撰写第 6 版时给我的帮助：

David Miller，他的工作热情、忠诚和友谊一直激励着我。能够与 David 共事，我觉得非常荣幸。没有他，我永远无法尝到龙舌兰酒的醇香。

Clement Dipuis，他待人热情，乐于助人，是一位不可多得的导师和朋友。

我公司的团队成员：Susan Young 和 Teresa Griffin，我无法表达对你们每个人深深的感激之情。

Greg Andelor，他是位图形艺术家，我这本书和我的其他项目很多图表都是出自他手，不幸的是他如此年轻就离我们远去了，我将永远怀念他。

Tom Modden 和 Randy Vickers，感谢他们为这本书写的精彩前言。

我的编辑 Tim Green 和我的出版合伙人 Stephanie Evans，他们在和我一起处理这些项目时总能耐心工作。

我最好的朋友和母亲 Kathy Conlon，即使她身体有时不太好，但总是陪伴在我身边。

特别是，我想要感谢我的丈夫 David Harris，谢谢他一直以来的支持与爱。没有他对我的坚定信心，我根本无法取得目前的成就。

前　言

我已经从事安全业务 39 年了，其中 26 年专注于信息安全。这些年我们已经看到了这个行业前所未有的变化：原来的计算机有一间屋子那么大，而且必须用水冷。到现在手机的计算能力已经超过了美国宇航局用于登陆月球所用的计算机。

我们敬畏地看着这一切，技术在发展，我们的生活质量也在不断提升。例如，我们可以通过手机来支付，我们的汽车也是计算机控制的，计算机控制带来了性能的优化和燃料的经济性，我们可以在酒店的房间办理登记手续并且得到登机牌。

但遗憾的是，一些人却通过技术和自己的优势找到漏洞，把这些进步变成了他们个人或其组织谋取政治利益和经济利益的工具。

为了应对这些对手，信息安全专业出现了。第一个认识到信息安全专业的组织是$(ISC)^2$，它成立于 1988 年。1994 年$(ISC)^2$创建了注册信息系统安全专家(Certified Information System Security Professional，CISSP)认证并举行了第一次考试。这样就可以给经理和雇主(和潜在的雇主)一个保证，证实证书持有人对组成公共知识体(Common Body of Knowledge，CBK)中的 10 个领域都有基本的理解。

Shon Harris 撰著的《CISSP 认证考试指南》(*CISSP All-in-One Exam Guide*)是为应考者准备 CISSP 考试的指导书籍。我看到过许多类似的考试指南，Shon 的书和别人的区别是她的书并不教人们如何通过考试，而是教你要通过考试所需的知识和材料。这意味着，虽然可能已经通过考试并获得证书，但是 Shon 的书仍然会在你的书架上(或平板电脑中)作为一个有价值的参考指南。

我认识 Shon 已经将近 15 年了，感动我的是她的奉献精神、道德和荣誉。她是我们这个行业里我遇到的最专业的人。她不断工作来改进她的书以便所有水平的读者都能理解各个主题。她开发了一种学习模式，帮助确保一个组织从底层到最高管理层的每个人都知道对他们负责的数据尽职尽责是明智的选择。

很荣幸有机会帮助介绍 CISSP。我是 Shon 的忠实读者，我认为学习完这本书之后，你也会成为 Shon 的忠实读者。享受这段学习经历，为了这个证书而付出努力将物有所值。

Tom Madden, MPA, CISSP, CISM
疾病控制中心首席信息安全官

当今，网络安全环境不断变化，我们在很多正常活动时，比如收发电子邮件、上网冲浪等，都会遭受攻击。敌人可能会一直通过手机应用、电子邮件(钓鱼、垃圾邮件)、网站(重定向)或者其他工具对我们的日常活动发起攻击，来获得知识产权、个人信息或其他敏感数据。黑客行动主义者、罪犯和恐怖分子通过使用上述信息实现未经授权地访问系统和敏感数据。

黑客行动主义者通常使用攻击期间收集的信息来传递他们的消息，达到他们的目标。据赛门铁克的报告，在 2010 年，发现 163 个与移动计算相关联的新漏洞，286 亿个恶意软件变种，网络攻击数量增加了 93%，260 000 个身份信息泄漏。据迈克菲的报告，在 2011 年的前两个季度出现了 16 200 个恶意网站，平均每天有 2600 个钓鱼网站出现。

我们也看到了在我们的日常活动中新技术在不断发展。新的智能手机和平板电脑已经成为常见的家用电脑。但是新工具往往意味着新的漏洞，网络安全专家必须处理。信息技术实施人员需要快速设计和实施。其中关于新技术讨论最多的很可能对整个系统或组织造成风险。CSO/ CISO 会与技术部门一起寻找运用新技术的最佳方法，但物理安全和网络安全是部署策略中非常重要的部分。

培训是非常重要的，可以帮助最终用户、网络安全从业者，高级管理层明白他们的行为对组织内部有什么影响。甚至技术人员在家远程办公，连接到企业网络或将数据带回家都可能产生严重的后果。安全策略的推行将帮助建立一个更强的安全基线。组织已经意识到这个问题，很多组织已经开始编写可实现可接受的网络使用策略。这些策略如果执行得当，将有助于减少网络安全事件的发生。

一个解决方案是不可能解决网络安全问题的。深度防御、最佳业务实践、培训和意识教育、及时的信息共享等技术可以使网络攻击的影响降到最低。网络安全专家们需要使领导层及时了解最新的威胁和减少这些威胁影响的方法。由首席财务官、首席执行官、首席运营官做出的许多日常行为和决定，将会对任务实现产生影响；安全决策也应该成为这个流程的一部分。

在我获得证书后，《CISSP 认证考试指南》一直是我的一本重要参考资料。Shon Harris 创作并继续完善着这本全面的学习指南。组织机构各个层面的人，特别是网络安全人员，应该努力获得 CISSP 认证。这本学习指南是成功获得这个认证的关键，是网络专家准备和获得 CISSP 的工具包。CISSP 的 10 个相关领域将协助个人从许多角度来认识信息安全。我们不再仅仅关注信息安全领域的一个方面，它为我们提供了多个视角，提供了专业的、总体的网络安全。从策略领域到技术领域，CISSP 和这个学习指南涉及了网络安全的方方面面。即使这不属于你目前的培训计划，这本书将帮助任何人成为一个更好的安全从业者并且改善他们的组织安全状况。

Randy Vickers
Alexa Strategies, Inc.
网络安全分析师和顾问
CERT 美国的前总裁，国防部 CERT(JTF-GNO)前首席

目　录