(ISC)² Official Study Guide

安全技术经典译丛

CCSP

官方学习指南

云安全认证专家

CCSP (ISC)² Certified Cloud Security Professional Official Study Guide

[美] 布赖恩·奥哈拉(Brian T. O' Hara) 著
本·马里索乌(Ben Malisow)
栾 浩 译
北京爱思考科技有限公司 审校

100%涵盖CCSP所有考试目标，全面讲解云数据安全、云应用安全、运营、合规等重要主题

SYBEX
清华大学出版社

安全技术经典译丛

CCSP 官方学习指南

云安全认证专家

[美] 布赖恩·奥哈拉(Brian T. O'Hara)
本·马里索乌(Ben Malisow) 著

栾 浩 译

北京爱思考科技有限公司 审校

清华大学出版社

北 京

Brian T. O'Hara, Ben Malisow
CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide
EISBN：978-1-119-27741-5

北京市版权局著作权合同登记号 图字：01-2017-5010

图书在版编目(CIP)数据

CCSP 官方学习指南　云安全认证专家 /(美) 布赖恩·奥哈拉(Brian T. O'Hara)，(美)本·马里索乌(Ben Malisow) 著；栾浩　译. —北京：清华大学出版社，2018
(安全技术经典译丛)
书名原文: CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide
ISBN 978-7-302-50570-9

Ⅰ. ①C…　Ⅱ. ①布…　②本…　③栾…　Ⅲ. ①计算机网络－安全技术－资格考试－自学参考资料　Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2018)第 141308 号

责任编辑：王　军　韩宏志
装帧设计：孔祥峰
责任校对：牛艳敏
责任印制：董　瑾

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：三河市国英印务有限公司
经　　销：全国新华书店
开　　本：170mm×240mm　　印　　张：18.5　　字　　数：400 千字
版　　次：2018 年 10 月第 1 版　　印　　次：2018 年 10 月第 1 次印刷
定　　价：98.00 元

产品编号：072583-01

译 者 序

在 2018 年 3 月召开的第十三届全国人民代表大会第一次会议上，李克强总理在政府工作报告中明确提出“深入开展‘互联网+’行动，实行包容审慎监管，推动大数据、云计算、物联网的广泛应用”。总理的讲话体现了国家层面对云计算的重视，可以预见，在今后相当长时期内，云计算将一直是热点领域。

自从 Google 首席执行官埃里克·施密特(Eric Schmidt)在 2006 年提出“云计算”概念以来，云计算技术历经十多年的迅猛发展，取得了长足进步。众多企业从起初的谨慎观望，转为热情拥抱云计算。各大厂商也不断推出各种云计算产品和服务。

按照 NIST(美国国家标准与技术研究院)的定义：“云计算是一种模式，是一种无处不在的、便捷的、按需提供的、基于网络访问的、共享使用的、可配置的计算资源(包括网络、服务器、存储、应用及服务)，可通过最少的管理工作或与云服务提供商的互动来快速配置并发布”。云计算是对信息技术架构的一场革命；未来，企业不需要建设机房、维护软硬件设备就能以经济实惠的价格获得强大的计算能力。

新技术也带来了新挑战。信息安全问题尤为突出：数据保存在企业外部，与其他公司共用系统和服务，由第三方人员管理维护，支撑云计算的数据中心可能位于另一个具有不同法律体系的国家，需要满足不同的个人隐私保护要求，面临严峻的合规挑战。

在安全行业，企业与攻击者攻防激烈，一直处于“道高一尺，魔高一丈”的缠斗状态。云计算技术的横空出世，将双方的战场转移到一片更广阔的天地。传统的安全信任边界变得模糊，政府、企业及个人如何识别可信的云计算服务提供商？如何保护云计算服务环境下的数据安全和隐私？如何评估云计算服务的整体安全性？如何更新自己的安全策略？这些都是全新的课题。

作为国际性安全行业观察者，$(ISC)^2$ 与 Cloud Security Alliance 及时捕捉到这一需求，推出 CCSP(云安全认证专家)课程及认证考试。CCSP 知识体系代表云计算安全知识和经验的业界最高标准，在全球范围内得到广泛认可，认证地位稳步上升。持有该证书，专业人员可证明自己具有扎实渊博的学识和深厚的造诣，掌握了国际公认的高级云安全专业知识，具备规划、设计、运维和服务能力。

本书全面系统地讲述 CCSP 认证考试的所有知识域。$(ISC)^2$ 假定 CCSP 认证的应试者透彻理解信息安全领域的基本知识，并具有一定的工作经验。本书不介绍基础内容，但这些在考试中是会出现的。如果你尚未通过 CISSP 等认证，最好首先补充学习一些 CISSP 认证的相关资料。另外，即使你暂不准备参加认证考试，但希望全面理解云计算安全相关知识，学习本书也将受益匪浅。

北京爱思考科技有限公司(Beijing Athink Co., Ltd)专门组织力量将该书翻译出版，

希望书中介绍的有关 CCSP 认证考试的内容能指导读者理解和掌握云计算安全知识，也能为 CCSP 考生进行学习和备考提供支持和帮助。

这里衷心感谢本书的原作者和编辑们，是他们的支持和授权，才使这本书的中文版得以顺利出版；还要感谢(ISC)²中国办公室和清华大学出版社将本书引入中国，以飨广大安全行业的读者；更要感谢为这本书的出版付出大量艰辛劳动的各位译者，是各位译者的辛勤工作，才使中国读者得以方便地学习 CCSP 中云计算安全的相关知识与经验；最后感谢清华大学出版社的王军老师及编辑团队，他们在编辑过程中严格把关，提出详尽的修订建议，保证了本书的绝对权威和上乘质量。

最后，预祝所有应试者顺利通过 CCSP 认证考试；衷心希望广大读者通过本书学到 CCSP 知识精髓，并在云计算信息安全领域做出一番辉煌事业！

译者简介

栾浩，获得上海大学项目管理专业管理学学士学位，持有 CISSP、TOGAF 9、CISA、CCSK、F5SE、ITILv3(F)、MCSE、MCDBA、ISO27001LA 和 BS25999LA 等认证，现任融天下互联网科技(上海)有限公司首席技术官(CTO)及首席信息安全官(CISO)职务，负责金融科技研发、云平台管理、信息安全、数据安全和风控审计等领域。栾浩先生是 2015-2017 年度(ISC)²上海分会理事。栾浩担任本书翻译工作的总技术负责人，负责统筹全书各项工作事务，并承担第 3 章的翻译工作，以及第 1、3、4、10、11 章的校对工作，以及本书同步材料的翻译工作和全书的审阅及定稿工作。

顾伟，获得上海外国语大学工商管理硕士学位，持有 CISSP、CCSP、CISP、CISA、CISM、CGEIT、CRISC、PMP、Cobit5(F)、ITILv3(F)、GIAC 和 CIPM 等认证，现任安进生物制药公司日本及亚太地区业务信息安全官，负责日本及亚太区域业务相关的数据安全、云计算安全、安全运维、安全架构、风险管理和隐私合规等领域。顾伟先生是 2017 年度(ISC)²亚太信息安全领袖、信息安全专业人士获奖者，是 2017 年度(ISC)²上海分会理事。顾伟负责本书第 5 章和第 9 章的翻译工作，第 1 章和第 3 章的审校工作，以及本书同步材料的翻译工作。

姚凯，获得中欧国际工商管理学院工商管理硕士学位，持有 CISSP、CCSP、CSSLP、CISA、CISM、CGEIT、CRISC、CEH、CIPT 和 CIPP/US 等认证，现任欧喜投资(中国)有限公司 IT 总监，负责信息科技、信息安全、隐私合规等领域。姚凯先生负责本书第 1 章的翻译，第 4 章和第 10 章的审校工作，并为本书撰写了译者序。

万鑫，获得华中科技大学计算机科学与技术专业博士学位，持有 CISSP、CISA、CCSK、DevOps Master、ISO27001/20000/22301LA 等认证，现任英国标准协会(BSI)中国区 ICT 技术总监，负责信息安全、IT 服务管理领域的对外培训和服务工作。万鑫负责本书第 2 章的翻译工作，以及本书同步材料的翻译工作。

胡妙超，获得上海交通大学通信与信息系统专业工学硕士学位，持有 CISSP、CCSP、CEH、CISM、CISA 和 HCIE-Cloud 等认证，现任中国大地财产保险股份有限公司安全主管，负责网络与信息安全管理领域。胡妙超负责本书第 7 章和第 8 章的翻译工作，以及第 5 章和第 6 章的审校工作。

唐文剑，获得中央财经大学工商管理硕士学位，持有 CISSP 和 CISA 等认证，现担任(ISC)²华南分会会长，负责 IT 治理、IT 风险管理、信息安全以及企业风险管理与内部控制等领域。唐文剑著有《区块链将如何重新定义世界》一书，唐文剑负责本书第 6 章和第 11 章的翻译工作，以及第 7 章和第 8 章的审校工作。

王向宇，获得安徽科技学院网络工程专业工学学士学位，持有 CCSK、CISP、软

件开发安全师和 CISP-A 等认证。现任京东集团企业信息化部高级安全工程师，负责日常安全事件处置与应急、安全监控平台开发与维护、云平台安全、SDLC 安全体系和内控审计等工作。王向宇先生负责本书第 4 章的翻译工作，第 2 章和第 9 章的校对工作，以及本书同步材料的翻译工作。

张伟，获得清华大学工商管理硕士学位，持有 CISSP 和 ITIL(F)等认证。现任北京初到科技有限公司 CEO 职务，负责云计算、人工智能等新技术领域。张伟负责本书第 10 章的翻译工作，以及第 9 章和第 11 章的审校工作。

雷兵，获得同济大学海洋地质专业理学硕士学位，持有 CISSP、CCSP、CISM、CISA 和 CEH 等认证，现任携程旅行网信息安全专家。雷兵负责本书第 1～3 章、第 6 章和第 11 章的通校工作，以及前言的部分翻译工作。

吴潇，获得中国科学技术大学信息安全专业硕士学位，持有 CISSP、CISA、PMP、ITILv3(F)和 ISO27001 等认证，现任北京天融信网络安全技术有限公司深圳分公司专家级安全顾问，日常负责信息安全技术服务、云平台安全、数据安全、等级保护和法律合规等领域。吴潇负责本书第 5～8 章的校对工作，本书第 4、5、7、8、9 章的通校工作，以及前言的部分翻译工作。

毛小飞，毕业于湘潭大学计算机系，持有 CISSP 和 ISO27001 等认证。现任京东集团企业信息化部渗透技术负责人，负责渗透测试、病毒分析、安全产品开发和应急响应等技术工作。毛小飞先生负责本书全部章节的技术勘误和最终技术审校工作。

最后，感谢$(ISC)^2$ 中国区顾问王新杰，$(ISC)^2$ 中国区总代理——北京爱思考科技有限公司的黄海波、李莉、许建名；感谢诸位安全专家在本书译校过程中的帮助，包括吕劼、朱毅、危国洪、廖勇、张东，以及$(ISC)^2$华南分会的杨雄、王建霞和李钰琳等。

作者简介

Brian T. O'Hara，持有 CISSP、CCSP、CISA 及 CISM 认证，担任 Do It Best 公司的信息安全官，拥有 20 多年的安全和审计工作经验，在 PCI、医疗、制造和金融服务行业提供审计和安全咨询服务，曾担任世界 500 强公司的信息安全官。在进入 IS 审计领域之前，Brian 曾担任美国最大的社区学院的信息技术项目主席一职，在那里他协助建立了美国国家安全局(NSA)第一个两年制的信息安全学术研究中心。除了参与撰写 *CISA Study Guide*，他还是 Wiley、Sybex 和$(ISC)^2$的技术编辑。10 多年来，Brian 在本地和国际信息安全系统协会(ISSA)都是活跃分子，也是 ISSA 会员。Brian 是 ISACA Indiana 分会的前任主席，以及 InfraGard Indiana 成员联盟的主席。InfraGard Indiana 成员联盟由 FBI 与私企合作成立，共同保护美国的关键基础设施。

Ben Malisow，持有 CISSP、CCSP、CISM 和 Security+认证，担任 CISSP 和 CCSP 认证课程的$(ISC)^2$官方讲师。Ben 在信息技术和信息安全领域工作了近 25 年。曾为 DARPA 编写过内部 IT 安全策略，担任过 FBI 最高机密的反恐情报共享网络的信息系统安全经理，并协助开发了美国国土安全部交通安全管理局的 IT 安全架构。Ben 任教于多所大学和学校，包括卡内基梅隆大学 CERT/SEI、UTSA、南内华达学院以及一所拉斯维加斯学校，为迷茫的年轻人提供 6 至 12 年级的课程。Ben 出版过多本信息安全著作，也曾为 *SecurityFocus.com*、*ComputerWorld* 和其他期刊撰稿。

技术编辑简介

Tom Updegrove，担任 CCSP 和 EC-Council 的安全培训讲师、Internetwork 服务公司的 CEO，也是 AWS 和 Microsoft Azure 的合作伙伴。Tom 拥有 20 多年的技术和安全服务工作经验，在 PCI、医疗、制造和金融服务领域提供安全咨询服务。除了为本书做出贡献外，他还在 Wiley 和 Sybex 担任安全相关书籍的技术编辑，并为 ITProTV 讲授社会工程课程。Tom 协助开发了 Liberty 大学 MIS 实验室的基础设施，目前也担任 *Hakin9* 和 *Pen Testing* 杂志的技术编辑。

Jerry K. Rayome，获得计算机科学学士及硕士学位，持有 CCSP 证书，是 Lawrence Livermore 国家实验室网络安全项目的成员。Jerry 拥有逾 20 年的网络安全服务经验，包括软件开发、渗透测试、事件响应、防火墙实施与审计、网络安全调查取证、NIST 800-53 控制实施/评估、云风险评估和云安全审计等方面。

致　谢

感谢(ISC)²，感谢优秀的 Sybex 发行与编辑团队，包括 Jim Minatel、Kelly Talbot、Rebecca Anderson 和 Christine O'Connor，正是这些杰出人士的辛勤努力促成了本书的出版。

本书献给所有准备参加 CCSP 认证的应试者，我们衷心希望本书能为 CCSP 应试者顺利通过考试带来帮助。

前　言

近年来，云计算改变了业界开展业务的方式。很多组织正在重新思考其 IT 战略，将云计算的概念和实践作为在当今市场竞争中赢得优势的一种方式。信息安全行业也已经认识到云计算在专业性、新颖性和颠覆性方面的独特优势，同时，行业对具备云安全知识和技能且经过正规培训的安全专业人员的需求量激增。

$(ISC)^2$ 与云安全联盟(Cloud Security Alliance，CSA)合作开发了 CCSP(Certified Cloud Security Professional，云安全认证专家)认证体系，恰好可以满足对训练有素的合格云安全专业人员的不断增长的需求。

本书将为云计算专业人员顺利通过 CCSP 考试打下坚实的知识基础。

本书面向学生和安全专业人员，经过学习并通过这项具有挑战性的考试，在职业生涯中进一步提升自己。

$(ISC)^2$

CCSP 考试由国际信息系统安全认证联盟(International Information Systems Security Certification Consortium)管理，该联盟的英文简称是$(ISC)^2$。$(ISC)^2$ 是一个全球性的非营利组织，其主要目标包括以下四个方面：

- 维护信息系统安全领域的公共知识体系(Common Body of Knowledge，CBK)；
- 为信息系统安全专业人员和从业人员提供认证体系；
- 开展认证培训并管理认证考试；
- 通过持续教育，监督对合格认证应试者的持续认证。

$(ISC)^2$ 从其已认证的安全从业者队伍中遴选董事会经营其日常业务，$(ISC)^2$ 支持并提供多项认证，包括 CISSP、SSCP、CAP、CSSLP、CCFP、HCISPP 以及本书描述的 CCSP 认证。这些认证旨在验证和审查跨行业的 IT 专业安全人员的知识和技能。CCSP 应试者可访问 www.isc2.org，获取有关该组织及其他认证的更多信息。

知识域

CCSP 认证涵盖 CCSP CBK 六个知识域的材料：

知识域 1：架构概念和设计要求

知识域 2：云数据安全

知识域 3：云平台与基础架构安全

知识域 4：云应用安全

知识域 5：运营

知识域 6：法律与合规

(ISC)² 与 CSA 一起梳理了上述知识域，涵盖了与云相关的所有安全领域。理解和掌握云计算每个领域的知识，可确保云安全专业人员能对涉及云计算所有功能和安全方面的问题，提供合理的建议和最佳实践。

更多相关信息，可访问(ISC)² 官方网站 www.isc2.org/ccsp。

考试资格和要求

(ISC)² 规定了申请 CCSP 认证必须达到的资格和要求，具体如下：

- 累积至少五年全职带薪的 IT 信息技术从业经验，其中三年必须工作在信息安全领域，并在 CCSP 考试的六个知识域之一具有一年经验。
- 获得云安全联盟的 CCSK 证书，可取代 CCSP 考试六个知识域之一的一年经验。
- 获得 CISSP 证书，可取代 CCSP 认证申请对工作经验的要求。

暂不具备这些要求的 CCSP 应试者仍可参加考试并申请(ISC)² 的准会员资格，在满足上述要求后，可申请获得正式会员资格。CCSP 应试者还必须遵守(ISC)² 正式道德规范，正式道德规范可在(ISC)² 网站 www.isc2.org/ethics 上找到。

CCSP 考试概述

CCSP 考试包含 125 道单项选择题，涵盖 CCSP CBK 的六个知识域。

CCSP 考试时间为 4 个小时。其中，有 25 个测试题目不计入最终得分，仅用于研究目的和开发新的试题和答案。考生无法知道哪些是测试题目，哪些是正式考题，所以请务必回答每个问题，每道未答题得 0 分。请以这种方式来分析：即使不知道答案，CCSP 应试者也有四分之一的机会选对正确选项，如果至少能排除两个不正确的答案，那么 CCSP 应试者就有一半的机会选对。所以，请务必回答每个问题。

CCSP 考题类型

CCSP 考试中的大多数问题是单项选择题，每题有四个选项，其中一个是正确答案。有些问题很直接，例如，要求 CCSP 应试者确认一个技术定义。而其他一些问题，则要求 CCSP 应试者识别一个适当的概念或最佳实践。这里有一个例子：

1. 将代码转换成一种即使获得了源代码也很难阅读和理解的形式，这项技术

被称为：

A. 随机化　　B. 弹性

C. 混淆(Obfuscation)　　D. 遮蔽(Masking)

CCSP 应试者需要选择正确或最佳答案。有时答案很明显，有时在两个好的答案之间进行区分并挑选最好的答案会更困难些。留意对一般、特定、通用、超集和子集答案的选择。在其他一些情况下，没有一个答案看上去是正确的。这时，CCSP 应试者需要选择不正确性最低的答案。还有一些问题是基于场景的，必须根据具体情况回答几个问题。

注意：

以上问题的正确答案是选项 C“混淆”。混淆是一种为防止未经授权查看而采用的代码转换技术。

除了标准的单项选择题格式外，CCSP 考试还包括一种图形拖放方式的题目格式。例如，CCSP 应试者可能在屏幕一侧看到需要拖放到屏幕另一侧相应对象上的项目列表。另一种交互式问题可能包括将术语与定义相匹配，并单击图表或图形的特定区域。这些交互问题的权重值比单选题高，在回答时应特别注意。

学习和备考技巧

本书建议 CCSP 应试者在 CCSP 备考计划中，进行至少 30 天的夜间密集学习。本书整理了一些实践方法，可加快 CCSP 应试者的复习进度。

- 花一两个晚上的时间仔细阅读每一章，完成最后的复习材料。
- 考虑加入一个学习小组。
- 回答所有复习题并参加模拟考试。
- 完成每章的书面实验题。
- 在开始下一部分工作之前，请务必温习前一天的工作，以防止遗忘信息。
- 可以留出一点休息时间，但要一直持续学习。
- 制订学习计划。
- 复习(ISC)² 考试大纲，即 www.isc2.org 网站上的 Exam Outline 文件。

提示：

本书建议 CCSP 应试者花费与完成模拟考试和学习一样多的时间来阅读和回顾概念。CCSP 应试者也可访问其他在线资源，如 www.cloudsecurityalliance.org 和其他专注于 CCSP 或云计算方面的网站。

考试格式和评分

CCSP 考试由 125 个单选题组成，每个题目有 4 个选项。可能还有基于场景的问题，可能有一个或多个与此场景相关的单项选择题。还有 25 个测试问题不计得分，这些仅用于研究目的，这是(ISC)² 开发新题目以保持考试包含最新内容的方式。考生不知道哪一个是测试题目，所以请回答所有问题。未作答的问题不会得分。

参加考试的建议

以下是一些考试窍门和一般原则：

- 先回答简单问题。CCSP 应试者可以标记不确定的题目，并在做完所有题目后再回头审查。
- 首先消除不正确的答案选项。
- 注意题目语言中的双重否定。
- 仔细阅读题目，确保完全理解题目的内容。
- 慢慢来，千万不要心急。匆忙和慌乱将导致考试焦虑和注意力不集中。
- 如果需要，可以去洗手间或休息一下，但要控制好时间。CCSP 应试者需要集中注意力。

管理好时间。考生有 4 个小时来回答 125 个问题。这相当于每个问题约两分钟，大多数情况下，时间是充足的。

确保 CCSP 应试者前一天晚上有充足的睡眠，并尽量少喝咖啡，以便在考试当天不会感到紧张。一定要带上 CCSP 应试者认为可能需要的食物或饮料，这些会在 CCSP 应试者考试时被储存在储物柜中。此外，请记得带上必备的药物，并提醒工作人员任何可能影响 CCSP 应试者考试的情况，如糖尿病或心脏病。健康比任何考试或认证都重要。

不可戴手表进入考场。计算机屏幕和考场内都有计时器。进入考场，CCSP 应试者还必须清空口袋，只能带储物柜钥匙和身份证件。

进入考点时，CCSP 应试者至少必须携带一张包含签名和照片的身份证件(如驾驶执照和护照)，还需要准备一份带签名的身份证件。确保 CCSP 应试者带齐所需材料，至少提前 30 分钟到达考点。带上 CCSP 应试者从考试中心收到的包含 CCSP 应试者 ID 的考试注册表。

如果英语不是 CCSP 应试者的第一语言，CCSP 应试者可注册其他几个语言版本的考试。如果需要翻译字典，CCSP 应试者必须能够证明自己确实需要，才可以使用。

完成认证过程

一旦 CCSP 应试者成功通过 CCSP 考试，在获得证书之前需要做几件事。首先，(ISC)^2 考试成绩会自动传送。当离开考试中心时，CCSP 应试者会收到打印的考试结果说明。成绩单将包括如何下载认证表的说明，认证表中会询问 CCSP 应试者是否已经拥有 CISSP 认证等类似问题。填写申请表后，CCSP 应试者需要签名并将表格提交给(ISC)^2 审批。通常情况下，CCSP 应试者会在几天内收到官方认证通知。一旦获得认证，CCSP 应试者可按(ISC)^2 使用指南的规定，在签名和其他重要的地方使用 CCSP 名称。

本书编排方式

本书涵盖六个 CCSP CBK 领域中的所有知识域，引导 CCSP 应试者清晰理解这些考试素材。本书正文由 11 章组成，内容如下：

第 1 章：架构概念
第 2 章：设计要求
第 3 章：数据分级
第 4 章：云数据安全
第 5 章：云端安全
第 6 章：云计算的责任
第 7 章：云应用安全
第 8 章：运营要素
第 9 章：运营管理
第 10 章：法律与合规 (第一部分)
第 11 章：法律与合规 (第二部分)

每章都包括旨在帮助 CCSP 应试者学习和测试的知识。建议先阅读第 1 章，然后转到其他章节，以便最好地了解主题。

注意：
请参阅目录和章节介绍，理解每章中涵盖的详细的知识域主题。

本学习指南的要素

本学习指南有几个要素，可帮助 CCSP 应试者为 CCSP 考试以及实际工作做好准备。

真实世界场景：本书提供了一些真实世界场景，通过查看某些解决方案在什么场合、在什么情况下在现实世界中起作用(或不起作用)以及为什么会如此，来帮助 CCSP 应试者进一步透彻理解相关信息。

小结：是对该章重要观点的概述。

考试要点：突出显示可能以某种形式出现在考试中的主题。虽然我们不确定特定考试将包含哪些内容，但本节强化了重要概念，这些概念对于理解 CBK 和 CCSP 考试规范至关重要。

书面实验题：每章包括书面实验室，汇集了该章提出的各种主题和概念。这些场景和问题提出了一些考虑因素，以协助 CCSP 应试者吸收知识，更好地理解和提出潜在的安全策略或解决方案。

复习题：每章都包括复习题，旨在衡量 CCSP 应试者对该章讨论的关键知识点的掌握程度。学完每章内容后可做一些复习题，如果不能正确回答某些题目，则表明 CCSP 应试者需要花更多时间学习相应的主题。章节练习题的答案在本书的附录 A 中。

章节特色和学习建议

本书有许多功能旨在指导 CCSP 应试者完成学习。每章开头列出该章涵盖的 CCSP 主题，让 CCSP 应试者快速了解全章内容。每章末尾有小结，然后是考试要点，旨在为 CCSP 应试者提供需要特别关注的快速提示项。最后，有几道书面实验题，这些实验将向 CCSP 应试者展示有关云问题和技术的实例，将帮助 CCSP 应试者进一步深刻理解相关材料。此处提出一些建议，以帮助 CCSP 应试者取得更圆满的学习效果：

- 在开始阅读前完成评估测试。这会让 CCSP 应试者了解需要花更多时间学习哪些知识域，以及哪些知识域只需要简单复习。
- 在阅读每章内容后回答复习题。如果回答不正确，请返回正文并查看相关主题。不看正文内容做练习题，检验自己的成绩如何。然后回顾复习错题中涉及的主题、概念、定义等，直到完全理解并熟练运用这些内容为止。

最后，如有可能，找一个学习伙伴或加入一个学习小组。与其他人一起学习和参加考试可能是一个很好的激励因素，大家也可以相互促进和提高。

评估测试

1. 哪种解决方案使企业或个人能使用存储服务提供商在互联网上存储他们的数据和计算机文件，而不是将数据存储在本地物理磁盘(硬盘驱动器或磁带备份)?

A. 在线备份　B. 云备份解决方案　C. 可移动硬盘　D. 遮蔽

2. 使用 IaaS(基础架构即服务)解决方案时，以下哪一项并非云客户的主要优势？

A. 可伸缩性　B. 计量服务

C. 能源和冷却效率　D. 所有权成本转移

3. _____重点关注安全和加密，防止未经授权的复制，仅给支付费用的人员分发。

A. 数字版权管理(DRM)　B. 企业数字版权管理

C. 位裂技术　D. 消磁

4. 以下哪项是正确的四种云部署模型？

A. 公有云、私有云、联合云和社区云

B. 公有云、私有云、混合云和社区云

C. 公有云、互联网、混合云和社区云

D. 外部云、私有云、混合云和社区云

5. 以下哪项是一个特殊的数学代码，允许加密硬件/软件进行编码，并解密一个加密的消息？

A. PKI　B. 加密密钥　C. 公钥　D. 遮蔽

6. 以下哪项列出了 STRIDE 威胁模型的六个正确组成部分？

A. 欺骗、篡改、抵赖、信息泄露、拒绝服务和特权提升

B. 欺骗、篡改、抵赖、信息泄露、拒绝服务和社会工程弹性

C. 欺骗、篡改、抵赖、信息泄露、分布式拒绝服务和特权提升

D. 欺骗、篡改、不可抵赖、信息泄露、拒绝服务和特权提升

7. 以下哪个术语能够保证一封特定的邮件确实是发送者创建并发送给特定收件人，并且特定接收人成功收到信息？

A. PKI　B. DLP　C. 不可抵赖　D. 位裂技术

8. 故意销毁用于加密数据的加密密钥的过程，它的正确术语是什么？

A. 密钥管理不善　B. PKI

C. 混淆　D. 加密擦除

9. 在联合身份管理环境中，谁是依赖方，他们做什么？

A. 依赖方是服务提供者，他们会使用身份提供者生成的令牌。

B. 依赖方是服务提供者，他们会使用客户生成的令牌。

C. 依赖方是客户，他们会使用身份提供者生成的令牌。

D. 依赖方是身份提供者，他们会使用由服务提供商生成的令牌。

10. 使用唯一标识符号替换敏感数据，这些标识符保留了有关数据的所有重要信息，同时又不损害其安全性，这个过程是什么？

A. 随机化　B. 弹性　C. 混淆　D. 标记化