(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

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，毕业于湘谭大学计算机系，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

11. 以下哪种数据存储类型关联或用于 PaaS(平台即服务)?

A. 数据库和大数据　　B. SaaS 应用程序

C. 表格　　D. 原生和块数据

12. 用于软件技术，将应用程序软件从执行它的底层操作系统中进行封装，这个术语是什么?

A. 虚拟机管理程序　　B. 应用程序虚拟化

C. VMWare　　D. SaaS

13. 以下哪项是为保护股东和公众免遭企业会计错误和欺诈行为而制定的立法?

A. PCI　　B. GLBA　　C. SOX　　D. HIPAA

14. 可以安全存储和管理加密密钥并用于服务器、数据传输和日志文件的设备，它是什么?

A. 私钥

B. 硬件安全模块(Hardware Security Module，HSM)

C. 公钥

D. 可信操作系统模块(Trusted Operating System Module，TOS)

15. 在云供应商名下的一种云计算基础设施，供公众开放使用，由企业、学术机构或政府组织拥有、管理和运营，它是?

A. 私有云　　B. 公有云　　C. 混合云　　D. 个人云

16. 当使用数据库的透明加密时，加密引擎驻留在哪里?

A. 在数据库应用本身　　B. 在使用数据库的应用中

C. 在连接到卷的实例上　　D. 在一个密钥管理系统中

17. 采用基于非数字类型或级别的风险评估的方法、原则或规则，是哪一种评估类型?

A. 定量评估　　B. 定性评估　　C. 混合评估　　D. SOC 2

18. 以下哪项最能描述 CSA CCM(云安全联盟云控制矩阵)?

A. 云服务提供商的一系列监管要求

B. 云服务提供商的一套软件开发生命周期要求

C. 一个安全控制框架，提供与主要行业认可的安全标准、法规和控制框架(如 ISO 27001/27002、ISACA 的 COBIT 和 PCI-DSS)之间的映射/交叉关系

D. 不同安全域中的云服务安全控制清单

19. 发生法律冲突时，_____确定将听取争议哪一方的管辖权。

A. 侵权法　　B. 准据法(Doctrine of Proper Law)

C. 普通法　　D. 刑法

20. 选择新的数据中心基础设置时，以下哪项是最重要的安全考虑因素?

A. 地方执法响应时间　　B. 与竞争对手设施相邻的位置

C. 飞机飞行路线　　D. 公用基础设施

21. 在云环境中清理电子记录时，以下哪一项总是安全的？

A. 物理破坏　　B. 覆写　　C. 加密　　D. 消磁

22. 以下哪项描述了 SYN Flood 攻击？

A. 快速传输 Internet 中继聊天(IRC)消息

B. 创建大量部分开放的 TCP 连接

C. 禁用 DNS(域名服务)服务器

D. 用户和文件的链接过多

23. 以下哪一项云存储形式，适于将个人的移动设备数据存储在云中，并为个人提供从任何地方访问数据的权限？

A. 原生存储　　B. 闪存　　C. 混淆归档　　D. 移动云存储

24. 以下哪个术语最能描述一个分布式模型，其中软件应用程序由供应商或云服务提供商托管，并通过网络资源向客户提供？

A. IaaS(基础架构即服务)　　B. 公有云

C. SaaS(软件即服务)　　D. 私有云

25. 以下哪项是美国颁布的一项联邦法律，用于控制金融机构处理个人隐私信息的方式？

A. PCI　　B. ISO/IEC

C. GLBA　　D. 消费者保护法

26. 安全无线应用协议(WAP)中，安全套接字层(SSL)的典型功能是保护_____的信息传输？

A. WAP 网关和无线端点设备之间　　B. Web 服务器和 WAP 网关之间

C. 从 Web 服务器到无线端点设备　　D. 无线设备和基站之间

27. 服务机构用哪一种关于控制方面的会计报告取代旧的 SAS 70 报告？

A. SOC 1　　B. SSAE 16　　C. GAAP　　D. SOC 2

28. 从云服务器托管商或云计算提供商处购买托管服务，然后转售给其自己客户的公司是？

A. 云代理商(broker)　　B. 云计算经销商(reseller)

C. 云代理(proxy)　　D. VAR

29. 依靠共享计算资源而不是使用本地服务器或个人设备来处理应用程序，可与网格计算相媲美的计算类型是什么？

A. 服务器托管　　B. 传统计算　　C. 云计算　　D. 内联网

30. 旨在分析应用程序源代码和二进制代码的安全性和脆弱性的一系列技术是？

A. 应用程序动态安全测试(DAST)　　B. 应用程序静态安全测试(SAST)

C. 安全编码　　D. OWASP

评估测试答案

1. B.　云备份解决方案使企业能使用存储服务，将数据和计算机文件存储在互联网上，而不是将数据存储在本地硬盘或磁带备份上。如果主要业务位置受损，导致无法在本地访问或恢复因为基础设施或设备受损而导致的本地数据，则云备份具有能提供访问数据的额外优势。在线备份和可移动硬盘是其他选项，但默认情况下不能为客户提供无处不在的访问。遮蔽是用于部分隐藏敏感数据的技术。

2. B.　可伸缩性、能源和冷却效率以及所有权成本转移都是采用 IaaS 的主要优势。

3. A.　数字版权管理(DRM)旨在将安全和加密作为一种手段，防止未经授权的复制和限制仅向经授权的(购买者)分发内容。企业数字版权管理也称为信息版权管理(IRM)，是 DRM 的一个子集，通常指企业对企业信息权的保护。位裂是跨多个地理边界隐藏信息的一种方法，消磁是一种从磁介质中永久删除数据的方法。

4. B.　唯一正确的答案是公有云、私有云、混合云和社区云。联合、互联网和外部都不是云模型。

5. B.　加密密钥是正确答案：用于加密和解密信息的密钥。加密密钥是数学代码，支持基于硬件或基于软件的加密系统对信息进行编码或解码。

6. A.　STRIDE 威胁模型中的字母表示身份欺骗、数据篡改、抵赖、信息泄露、拒绝服务和特权提升。其他选项只是混淆或不正确的版本。

7. C.　抗抵赖/不可抵赖是指特定的作者或用户不能驳斥或否认他创建和/或发送了一条消息，并且数据或消息的接收者不能否认他们已收到该消息。

8. D.　加密擦除的行为意味着破坏最初用于加密数据的密钥，从而使数据永远无法恢复。

9. A.　身份提供者将拥有所有身份并为已知用户生成一个令牌。依赖方(RP)将是服务提供者，并且会使用令牌。其他答案都不正确。

10. D.　用唯一标识符号代替敏感数据称为标记化，这是通过替换唯一标识符号隐藏敏感数据的一种简单且唯一有效的方式。它不像加密那样强大，但可以有效地防止敏感信息被窥视。虽然随机化和混淆处理也是隐藏信息的手段，但它们的表现完全不同。

11. A.　PaaS 使用数据库和大数据存储类型。

12. B.　应用程序虚拟化从应用程序执行的底层操作系统中封装应用程序软件。

13. C.　SOX(萨班斯-奥克斯利法案)是应对导致安然破产的 2000 年会计丑闻而颁布的。当时，高层管理人员声称他们不了解会导致公司倒闭的会计惯例。SOX 不仅强制管理人员监督所有的会计实践，而且如果类似安然这种事件再次发生，他们将为此负责。

14. B.　硬件安全模块是一种可安全地存储和管理加密密钥的设备。这些可用于服务器、工作站等。常见的类型称为可信平台模块(TPM)，可在企业工作站和笔记本上找

到。没有可信任操作系统模块这样的术语，公钥和私钥是与 PKI 一起使用的术语。

15. B.　这是公有云计算的定义。

16. A.　在透明加密中，数据库的加密密钥存储在数据库本身的引导记录中。

17. B.　定性评估是一套基于非数字类别或水平的风险评估方法或规则。使用这些数字类别或级别的称为定量评估。混合评估不存在，SOC 2 是关于控制有效性的会计报告。

18. C.　CCM 交叉引用了许多行业标准、法律和准则。

19. B.　如果对听审案件使用哪个司法管辖区存在争议，将使用准据法原则。侵权法是民事责任诉讼。关于婚姻的法律是普通法，而刑法涉及违反州或联邦刑法。

20. D.　在给出的答案中，选项 D 最重要。任何数据中心设施都必须靠近健全的公用基础设施资源，如电力、供水和网络连通性，这一点至关重要。

21. C.　由于云环境访问和物理分离的因素，可能无法实现物理破坏、覆写和消磁，但加密总是可以在云环境中使用。

22. B.　SYN Flood 在正常 TCP 连接尝试完成之前中断，从而让服务器等待响应。如果这些连接尝试数量庞大，则发生“泛洪”，导致终端单元消耗资源，服务和/或系统本身变得不可用。其他选项与任何类型的泛洪都没有关系。

23. D.　移动云存储被定义为一种云存储形式，适于将个人的移动设备数据存储在云中，并为个人提供从任何地方访问数据的权限。

24. C.　这是 SaaS(软件即服务)服务模式的定义。公有云和私有云是云部署模型，IaaS(基础架构即服务)不提供任何类型的应用程序。

25. C.　GLBA 针对的是美国的金融机构，并要求他们专门保护账户持有人的私人信息。PCI 是信用卡的处理要求。ISO/IEC 是一个标准化组织。消费者保护法虽然在保护消费者私人信息方面提供了监督，但范围有限。

26. C.　SSL 的目的是加密两个端点之间的通信信道。在这个例子中，它是最终用户和服务器。

27. B.　SOC 1 和 SOC 2 都基于 SSAE 16 标准，该标准替代了 SAS 70 标准。

28. B.　云计算经销商购买托管服务，然后转售它们。

29. C.　云计算建立在网格计算模型的基础上，有资源池可以共享，而不是让本地设备执行所有计算和存储功能。

30. B.　应用程序静态安全测试(SAST)与应用程序动态安全测试(DAST)的不同之处在于，它会查看源代码和二进制文件，确定能否在代码加载到内存中并运行之前检测到问题。

目　录

第 1 章

架构概念

本章旨在帮助读者理解以下概念：

✓ 知识域 1：架构概念和设计要求

- A. 理解云计算概念
  - A.1 云计算定义
  - A.2 云计算角色
  - A.3 关键云计算特性
  - A.4 构建块技术
- B. 描述云参考架构
  - B.1 云计算活动
  - B.2 云服务能力
  - B.3 云服务目录
  - B.4 云部署模型
  - B.5 云特点的相关考虑
- D. 理解云计算安全的设计原则
  - D.3 成本/效益分析

✓ 知识域 3：云平台与基础架构安全

- D. 规划灾难恢复和业务连续性管理
  - D.1 理解云环境
  - D.2 理解业务需求

✓ 知识域 6：法律与合规

- B. 理解隐私问题和司法管辖权的差异
  - B.3 机密性、完整性、可用性和隐私之间的差异

警告：
本章是本书其他章节的基础。在阅读其他章节前，先学习本章的知识点是非常有益的。

云安全认证专家(Certified Cloud Security Professional，CCSP)不是一项基础的计算机技能认证或培训；CCSP 面向云计算安全领域，是具有一定行业背景的从业人员的专业化认证。(ISC)^2 希望那些想要获得这项专业认证的人士，目前已在业界具有一定经验，从事信息安全相关工作，已经具备一定的专业能力，并深入透彻地理解计算机、网络、安全、业务和风险等相关领域的基本知识。(ISC)^2 期待参加该项考试的人士，已经持有其他可证明 CCSP 应试者专业知识和行业经验的认证证书，如 CISSP 认证等。因此，本书未涵盖应试者应该掌握的一些基础安全知识，但要注意，CCSP 考试范围将覆盖这些基础的安全知识。如果 CCSP 应试者没有 CISSP 认证背景，最好学习一些与 CISSP 认证相关的资料，来扩大自己的知识范围。

然而，CCSP 通用知识体系(Common Body of Knowledge，CBK)包含的术语和概念用特定方式进行表述。其中一些表述方式可能是 CCSP 认证所独有的，与 CCSP 应试者在日常 IT 运营中所用的术语和概念有所不同。因此，本章是一个指南，为帮助你理解云计算的特定知识和 CCSP CBK 的整体知识奠定基础。

云计算意味着很多知识内容，但是，以下这些特性已成为普遍接受的云计算定义的一部分：

- 广泛的网络接入
- 按需自助服务
- 资源池
- 可测量/可计量的服务

NIST 在云计算的定义中对这些特性进行了简洁的阐述。

NIST 800-145 云计算定义

NIST 给出的“云计算”官方定义是：“云计算是一种模式，是一种无处不在的、便捷的、按需的、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。”

上面提及的每个知识点都会出现在本书、CCSP CBK 以及考试中。

广泛的网络接入意味着永远不应出现网络带宽瓶颈。这通常是通过使用先进的路由技术、负载均衡技术、多站点托管(Multisite Hosting)和其他技术实现的。

按需自助服务指这样一个模型：允许云客户和云服务提供商之间，事前或事中不进行任何沟通，在很少交互或没有云服务提供商介入的情况下，云客户就可以扩展其计算和/或存储需求。这项服务是实时生效的。

资源池这个特征允许云服务提供商既能满足云客户的各种资源需求，又保持经济可行性。云服务提供商进行资本投资(Capital Investment)，该投资远超任何单一云客户可自行提供的资金；云服务提供商可按需分配这些资源，以免资源得不到充分利用(这意味着投资浪费)或被过度使用(这意味着服务水平的下降)。

最后介绍**可测量/可计量的服务**，简言之，意味着云客户仅支付与实际使用的资源相关的费用。这项服务像一家自来水公司或电力公司每月收取客户的水电费。

ISO/IEC 标准(ISO/IEC 17788，www.iso.org/iso/catalogue_detail?csnumber=60544)简要介绍云计算并列出了词汇。ISO/IEC 标准不仅包括上述特性，还增加了多租户(Multitenancy)特性。多租户特性虽然是大多数云服务产品的组件，但并非云计算服务领域的必然特性。有些云服务模型不包括多租户，因为云客户可购买、租用/租赁完全独占的资源。

下面将更详细地讨论所有这些概念。

真实世界场景

网上购物

想一想年底假日前零售行业销售旺季的 IT 需求。这段时间的购物客户数量和交易量都远超平日。这种情况下，通过在云中托管销售业务的 IT 能力，在线购物零售商可获取巨大好处。云服务提供商通过分配必要的资源以满足这一快速增长的突发 IT 需求，并将依据协议价格收取这部分新增 IT 能力的相关使用费用。当节日过后销售量下降时，零售商将不再需要继续支付这笔较高的费用。

这是一种很好的商业模式。因此，也有人说云计算不是技术驱动的，而是商业驱动的。

1.1　业务需求

IT 部门不是利润中心，而是提供支持的部门。信息安全部门亦如此。信息安全活动实际上会对业务效率造成阻碍(一般情况下，设备和流程越安全，效率就越低)。因此，是组织的业务需求驱动安全决策，而不是安全决策驱动业务需求(Business Requirements)。

成功的组织会尽可能多地收集与业务运营相关的需求信息。这些业务运营信息有多种用途，包括用于安全领域中的若干方面(本书将列举一些有关业务连续性/灾难恢复工作、风险管理计划和数据分类的案例)。同样，优秀的信息安全从业人员需要尽可能理解组织的运营状况。无论信息安全人员的级别或角色是什么，理解组织的运营状况都能帮助安全人员更好地执行安全任务。例如：

- 网络安全管理员必须根据组织业务来确定所需的通信流量类型。
- 入侵检测分析人员必须理解组织在做什么、为什么做、如何做以及在哪里做，以便更好地理解外部攻击的性质和强度，并相应地调整安全基线。
- 安全架构师必须理解组织的各个部门如何在不违背安全规范的情况下提升运营能力。

功能需求(Functional Requirements)：设备、流程或员工为完成业务目标所需的要素。例如，现场销售人员必须能远程连接到组织的网络。

非功能需求(Non-functional Requirements)：尽管不是设备、流程或员工完成业务目标所需的要素，却是希望满足的一些附加要素。例如，销售人员的远程连接必须是安全的。

许多组织目前正考虑将传统网络迁移到云端运营。这不是一个轻易的决定，这种转型必须能很好地支持业务需求。如前所述，云计算也有各种不同的服务和交付模式，组织必须决定使用哪一种服务和模式，才能帮助组织成功地实现业务目标。

1.1.1　现有状态

在云迁移之初，至关重要的是对业务流程、业务资产和业务需求进行切实的评估和理解。如果不能全面准确地掌握业务需求，在云迁移完成后，可能导致组织在新的云环境中出现业务流程失败、业务资产缺失或运营能力下降的情况。

然而，在开始云迁移工作时，组织的首要目标并不是确定使用哪种云服务模型最能够满足业务需求，而是确定组织的业务需求到底是什么。组织必须持有一份完整的资产、流程以及需求清单，在实践中，组织可采用多种方法来收集业务需求数据。通常，混合使用几种方法可防止遗漏。

收集业务需求的方法包括：

- 采访业务职能经理
- 采访用户
- 采访高级管理层
- 调查客户需求
- 收集网络流量
- 清点资产
- 收集财务记录
- 收集保险记录
- 收集市场数据
- 收集强制性合规要求

收集到足够的数据后，必须详细分析这些数据。这是业务影响分析 (Business Impact Analysis，BIA)工作的起点和基础。

BIA 是对组织内部每项资产和流程进行评估并赋予优先级的过程。正确的分析应当考虑每项资产受损或缺失将对整个组织的作用/影响。分析过程中，应特别注意识别关键路径和单点失败情况。此外，还需要确定需要付出多少成本才能满足法规，即针对组织业务的强制性法律监管和合同的要求。组织的监管法规取决于诸多因素，包括

组织所在的地区、组织所在的行业、客户的类型和所处的地理位置等。

注意：

资产可以是有形的(Tangible)或无形的(Intangible)。这些资产包括硬件、软件、知识产权、人员和流程等。例如，路由器和服务器就是有形资产。而无形资产常是无法触及的，例如，著作权、专利、商标、商业方法和商业秘密。

1.1.2　收益量化和机会成本

一旦通过业务线和流程清晰地理解了组织所从事的工作，就可以更好地理解组织可能从云计算迁移活动中获得的收益，以及与云迁移活动相关的成本。

显然，目前组织向云端迁移的最大动力是节省成本，这是一个非常重要且合理的想法。下面将介绍其中一些考虑因素。

1. 减少资本性支出(Capital Expenditure，CapEx)

如果组织购买了用于内部环境的某台设备，设备能力往往使用不足(能力闲置)，无法在所有时段都有效使用。而且，如果对该设备的能力需求有小幅上升，将可能使该设备的能力超出负荷，无法满足突发的使用要求。即便设备的能力没有得到充分使用，组织依然需要为没有使用的那部分额外能力付费。设备能力的闲置或剩余会产生浪费。

实际上，由于设备是一个整体，组织无法购买设备的一半或一部分，因此，除非组织甘冒风险将设备能力利用到接近超载(Overloading)的地步，否则，就一定会为该设备支付多余的费用。

但在云计算环境中，组织仅需要支付实际使用的资源的费用(不需要考虑处理负载所需的设备或部分设备的数量)，不再有额外的费用支出。这就是前面描述的“可计量”服务特性。结果，组织并没有对这些资产支付额外的费用。云服务提供商拥有更多额外的能力可以分配给云客户，因此，组织总能从容应对需求的增长(有些需求增长是巨量的、快速的和非常明显的)，而不会不知所措。

组织使用托管云服务的一种情况是在需求增加时，利用托管服务增强内部私有数据中心的处理功能。这种情况称为“云爆发(Cloud Bursting)”。该组织可能拥有自己的私有数据中心，但数据中心无法在高需求(紧急情况、拥挤的假日购物时段，等等)期间处理快速增长的需求，因此，组织的私有数据中心可根据需要向外部云服务提供商临时租用额外的能力，如图 1.1 所示。

因此，在迁移到云计算环境时，组织可立即实现成本节约(不需要为未使用的资源支付费用)，并避免代价高昂的业务风险(由于业务需求增长，导致服务失败的可能性加大)。

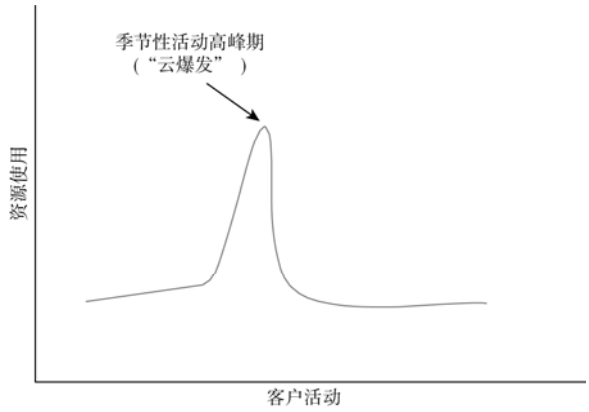

图 1.1　按需分配的弹性特性允许云客户定制资源的使用量

2. 降低人工成本

除了提供专业 IT 服务的公司之外，大多数组织的数据管理能力都不是核心能力，更非可以盈利的业务线。数据管理也是一种非常特殊的 IT 能力，雇用经验丰富且经过相关专业培训的 IT 员工相比其他职能部门的员工更昂贵，为满足内部 IT 环境需求雇用员工是组织的一项重要却不实惠的大型投资。迁移到云端后，组织即便不大量裁减高薪的 IT 员工，也可在很大程度上降低这些资深 IT 员工的雇用比例。

3. 减少运营性费用

维护和管理内部环境需要花费大量的精力和费用。当一个组织的 IT 系统迁移到云端时，IT 成本将转化为使用云计算服务的日常运营费用，可通过计算来精确支付。因此，成本由合同约定的统一汇总的费率进行计价，而非因为运营活动强度的增加(计划更新、紧急响应活动等)而增加。

4. 转移部分监管成本

一些云服务提供商可能为云客户提供全面的、有针对性的合规服务套餐。例如，云服务提供商可能拥有一组可应用于特定行业客户的安全控制项，以确保满足支付卡行业(PCI)的强制监管要求。任何希望得到该服务套餐的云客户都可在服务合同中约定，而不需要为单一控制项单独付费。云客户可通过这种方式减少一些工作并降低费用，否则，他们可能需要为遵守相关的规章制度而制定一个单独且昂贵的控制框架和安全体系。

提示：

后续章节将详细介绍服务水平协议(SLA)或服务合同(Contract)。

这里需要特别注意的是(本书也将反复强调)，根据现行法律，任何云客户都不能将无意或恶意泄露个人身份信息(Personally Identifiable Information，PII)相关的风险或责任转嫁给第三方。

这是非常重要的：如果组织持有任何类型的个人身份信息，就要对该数据的任何违规/泄露承担最终的全部责任，即便是使用了云计算服务且由于云服务提供商的疏忽或遭受攻击所造成的数据违规/泄露。

在法律和财务等各个方面，组织都需要对任何未经计划的个人身份信息泄露承担责任。

注意：

无论监管是来自法律还是合同义务，个人身份信息都是法律合规的一个重要组成部分。保护个人身份信息将是我们在云计算安全方面一项非常重要的考虑因素。

5. 减少数据归档服务/备份服务的成本

异地备份是长期数据归档(Data Archival)和灾难恢复的标准做法。即使一个组织不在云端执行常规操作，为“异地备份”采用云服务也是非常明智且有较好成本收益的选择。但结合使用归档/备份时，将操作移到云端可产生更大的规模效益，这会使组织从整体上节约成本。正如本书后面将讨论的，这也可增强组织的 BC/DR(Business Continuity/Disaster Recovery，业务连续性/灾难恢复)战略。

1.1.3　预期影响

可以计算出所有这些收益的金额。每种潜在的成本节约措施都可进行量化分析。高级管理层从业务专家那里获取这些信息，来平衡潜在的财务收益和云端运营的风险。

这个“成本效益”计算由“业务需求”驱动，并考虑安全因素；可供高级管理层决定将组织的运营环境迁移到云端是否合理。

注意：

大量风险与云迁移是密切相关的，本书将详细讨论这些问题。

1.2　云计算的演化、术语和定义

云计算的到来及其相关技术为我们提供了诸多优势。要将云计算和这些优势结合起来，就必须理解新术语，以及这些术语如何与传统模型的术语相关联。这些新技术及其术语是理解云计算服务模型和部署模型的组成部分。

1.2.1　新技术、新选择

15 年前，甚至 10 年前，如果建议组织将数据和 IT 运营交给一个在相距遥远的第三方服务团队，而且这个第三方服务团队组织管理层永远见不到，将被认为是一种绝对不能接受的风险。从信息安全角度看尤其如此：将控制权拱手让给外部供应商的做法是令人望而生畏的。然而，如今已将技术能力和基于合同的信任关系完美结合在一起，使得云计算不仅具有技术吸引力，而且从财务可行性来看，云计算几乎是一种必然的选择。

云计算具有一些标志性的特性。本节将定义这些特性，并逐一举例说明。

- **弹性(Elasticity)：**这是一种灵活性，当需要立即使用资源时，可按需分配资源，而不是按照其他因素来购买资源。例如，传统组织可能为每个员工购买一个台式机。在这个传统模型中，组织将购买台式机的全部能力，包括处理能力和存储容量等，即便每个用户在任何时候都不可能使用每台设备的全部能力。

  在云计算环境中，组织购买的不是一台(套)设备，而是要使用的服务能力。云服务提供商提供此类服务(同时还能获利)的能力依靠的是近年来的技术进步，包括虚拟化技术等提供的弹性和灵活性(后续章节进一步讨论虚拟化技术)。通过虚拟化技术，云服务提供商可在云用户和云客户需要时，将每个资源的部分使用权分配给每一个云用户和云客户，做到正好够用，不多也不少，进而避免浪费、资源闲置以及额外的非生产性成本。

  在虚拟化环境中，云用户还可从几乎任何设备或平台、几乎任何物理位置访问他们的数据。这将带来远远超出以前企业传统环境的可移植性、可用性和可访问性。
- **简单化(Simplicity)**：云服务的使用和管理对云客户和云用户是透明的。从云客户和云用户的角度看，数据服务已经支付过费用，是可以任意使用的，除了要履行职责中必需的部分外，很少需要额外信息。设计优良的云计算环境并不需要云服务提供商和云客户之间经常或频繁地进行互动。
- **可伸缩性(Scalability)**：组织的计算能力需求会发生变化；随着组织的不断成长，将不断拥有新的和更多的用户、客户和数据。在无须投入额外资金的情况下，云服务提供商就可以给云客户分配新的计算资源，而不需要增加成本。无论暂时还是长期，云计算服务都可通过比传统环境更廉价、更具成本效益的方式轻松地满足这些需求。

云客户(Cloud Customer)和云用户(Cloud User)之间的区别

云客户是任何购买云服务的人，可以是个人或公司。云用户只是使用云服务的人，可能是作为云客户的公司的雇员或者只是个人。

例如，公司 A 从云服务提供商 X 公司购买 SaaS 服务，那么 A 公司是云客户。A 公司的所有雇员都是云用户，因为他们使用了云服务，他们的雇主作为一个云客户，

已经购买了 SaaS 服务供他们使用。

不过，并非所有云用户都是云客户的员工。许多云用户只是个人，他们基于个人目的使用公有云服务，例如拥有 Gmail 账户的个人，或者把智能手机数据同步到免费的在线备份服务的个人。

1.2.2　云计算服务模型

根据云计算服务提供商提供的服务和云客户的需求，以及服务合同中双方的责任，云计算服务通常使用三种通用模型。这三种模型包括：基础架构即服务(Infrastructure as a Service，IaaS)、平台即服务(Platform as a Service，PaaS)和软件即服务(Software as a Service，SaaS)，如图 1.2 所示。本节将依次讨论这三种模型。

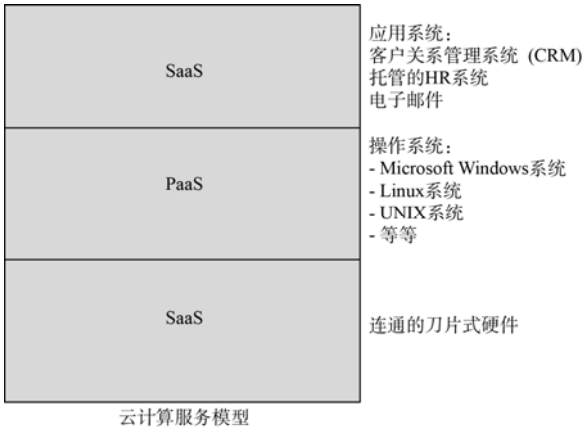

图 1.2　云计算服务模型

注意：

一些基于传统技术的供应商和顾问为使产品更具吸引力，在利用“云”概念方面不遗余力，将这个词融入他们能想到的每个术语中。我们看到诸如网络即服务(Networking as a Service，NaaS)、合规即服务(Compliance as a Service，CaaS)和数据科学即服务(Data Science as a Service，DSaaS)的被滥用的标签，但这些伪 XaaS 服务大多只是营销技巧；我们将这种情况称为云洗白(Cloud Washing)。不管是考试还是作为安全从业人员，都只需要知道 IaaS、PaaS 和 SaaS 这三个服务模型。

1. IaaS 模型

IaaS 模型是最基本的云服务产品，允许云客户在云服务提供商所管理和连接的硬件上安装所有软件，包括操作系统(OS)。

在该模型中，云服务提供商拥有带有机架、机器、线缆和公共设施的数据中心，

并管理所有这些基础架构的物理资源。但诸如软件的所有逻辑资源都由云客户自行管理。

从传统的角度看，组织可能认为这是 BC/DR 计划中的“温站(Warm Site)”：完备可用的物理空间，测试正常的网络连接；云客户的组织可使用任何类型的基线进行配置，并加载业务需要的任何数据。

对于希望增强数据安全控制权的组织，或在云端实施有限用途(如 BC/DR 或归档)的组织来说，IaaS 可能是最适用的模型。

IaaS 模型的案例包括提供 IaaS 的数据中心，数据中心允许云客户加载他们选择的任何操作系统和应用系统。云服务提供商只提供计算、存储和网络功能。

2. PaaS 模型

PaaS 模型包含IaaS模型中的所有内容，加上操作系统。云服务供应商(Cloud Vendor)通常提供可供选择的操作系统，以便云客户使用任意或所有的选项。云服务供应商将负责在需要时对系统打补丁，负责管理和更新操作系统，云客户可安装任何合适的应用软件。

PaaS 模型对于软件开发与运维一体化(DevOps)特别有帮助，因为云客户可在相对独立的环境中测试其软件，而不会破坏生产环境的功能，并可在不同操作系统平台上测试软件的适用性。

PaaS 模型的案例包括托管服务提供商，提供商不仅提供基础架构，而且加载了已加固的操作系统平台(如 Windows 服务器或 Linux 服务器)。

3. SaaS 模型

SaaS 模型包括前两个模型中列出的所有内容，额外添加了软件程序。云服务供应商也负责管理和更新软件。云客户基本上只负责在云服务提供商提供的完整生产环境中上传和处理业务数据。

我们可看到许多不同功能的 SaaS 模型配置案例。例如，Google Docs、Microsoft Office 365 和 QuickBooks Online 都是 SaaS 模型的产品。

SaaS 模型的一些案例包括客户关系管理(CRM)软件或运行在云端的会计软件。云服务提供商负责所有基础架构、计算和存储需求，还提供底层操作系统和应用系统本身。所有这些服务对最终用户是完全透明的，最终用户只看到他们购买的应用。

1.2.3　云部署模型

除了根据服务层次的不同来观察云产品外，还可从所有权的视角观察模型。下面将讲解两组模型各方面的情况。

1. 公有云

讨论云服务提供商时，通常想到的是公有云(Public Cloud)。资源(包括硬件、软件、设施和工作人员)都由云服务提供商拥有和经营，并出售或租赁给任何人(这就是公有云名称的由来)。

公有云服务提供商的案例包括 Rackspace、Microsoft Azure 和 Amazon AWS 服务。

2. 私有云

私有云(Private Cloud)是由组织独立拥有和运营的，是专供组织自己的云客户和云用户使用的云计算私有环境。私有云可被视为通过 Web 方式和远程访问功能连接的传统 IT 环境。如果你的组织承载 Web 服务器并允许通过远程服务访问，则可以将其视为私有云的实例。

私有云的案例包括过去被称为内联网(Intranet)的内部系统，通常是托管形式，托管内部共享的应用系统、存储和计算资源。一个实例是内部托管的 SharePoint 站点。

注意：

我们可能根据谁提供(而不是谁使用)来考虑“公有”和“私有”，因此这两个概念可能令人混淆。请记住，公有云由特定公司拥有，根据合同提供公共服务，而私有云由特定组织拥有，仅允许该组织授权的云用户使用。

3. 社区云

社区云(Community Cloud)是由追求共同目的或利益的多个组织拥有和运营的基础架构和处理能力；不同的部分可能由不同的个体或组织拥有或控制，但这些部分以某种方式聚集在一起，以执行联合的任务和功能。

游戏社区可能被视为典型的社区云。例如，PlayStation 网络涉及许多不同的实体参与在线游戏：索尼托管网络的身份和访问管理(IAM)任务，特定的游戏公司可能托管一系列服务器，运行数字版权管理(DRM)功能并处理某一游戏，而个人用户在自己本地的 PlayStation 上处理任务和存储。

4. 混合云

混合云(Hybrid Cloud)显然包含其他模型的各项元素。例如，组织可能希望保留某些私有云资源(例如，组织的用户可远程访问的传统产品环境)，也会租用一些公有云空间(可能是一个用于 DevOps 测试的 PaaS 模型功能，用来与生产环境相区分，从而大大降低系统崩溃的风险)。

混合云环境的一个案例是托管的内部云，例如一个 SharePoint 站点的一部分是为需要访问共享服务的外部合作伙伴划出的。对合作伙伴而言，这是一个外部云。因此，这将是混合运营的。

1.3　云计算中的角色和责任

参与云计算服务的不同实体包括：

云服务提供商(Cloud Service Provider，CSP)是提供云计算服务的供应商。CSP 将拥有数据中心、雇用员工、拥有和管理(硬件和软件)资源、提供服务和安全，并为云客户和云客户的数据及处理需求提供管理方面的帮助，例如 AWS、Rackspace 和 Microsoft Azure。

云客户(Cloud Customer)是购买、租赁或租用云服务的组织或个人。

云访问安全代理商(Cloud Access Security Broker，CASB)是第三方的实体，通常作为一个中介为云服务提供商和云客户提供独立的身份和访问管理(Identity and Access Management，IAM)服务。CASB 可采取多种服务形式，包括单点登录(SSO)、证书管理和密钥托管(Cryptographic Key Escrow)。

监管机构(Regulator)确保组织遵循规章制度框架。这些监管机构可以是政府机构、认证机构或合同的当事方。法律法规包括：健康保险流通和责任法案(Health Insurance Portability and Accountability Act，HIPAA)、格雷姆-里奇-比利雷法案(Graham-Leach-Bliley Act，GLBA)、支付卡行业数据安全标准(PCI-DSS)、国际标准化组织(ISO)、萨班斯-奥克斯利法案(Sarbanes-Oxley Act，SOX)，等等。监管机构包括联邦贸易委员会(FTC)、证券交易委员会(SEC)和委托审查合同或标准(如 PCI-DSS 和 ISO)合规情况的审计师，等等，这里不一一列举。

1.4　云计算定义

因为云计算的相关定义是理解后续章节的核心，并且是 CCSP 的基础安全知识，因此，本节介绍其中一些定义：

Apache Cloud Stack 是一个开源的云计算和 IaaS 模型平台，通过在云环境中提供一组相关的功能和组件，允许更方便地创建、部署和管理云服务。

业务需求(Business Requirement)是云计算迁移决策的驱动因素，也是风险管理的输入项。

云计算 APP 即云计算应用系统，用于描述通过互联网访问的软件应用系统，可能是用户设备上安装的代理或小程序。

云计算架构师(Cloud Architect)是云计算基础架构设计和部署专家。

云备份(Cloud Backup)将数据备份到基于云的远程服务器。作为云存储的一种形式，云备份的数据以一种可访问形式存储在组成云环境的多个分布式资源中。

云计算(Cloud Computing)是一种计算方式。与网格计算(Grid Computing)相比，云计算依赖可保证的计算资源(而不是本地服务器或个人设备)来处理应用系统。云计

算的使用目标通常是为军事和研究设施服务，具有与传统的超级计算机或高性能计算相匹配的计算能力，执行每秒数万亿次的计算，支持面向云客户的应用系统(例如金融投资组合)，甚至提供个性化信息或支持逼真的电脑游戏。

云计算经销商(Cloud Computing Reseller)从云计算服务器托管商或云计算提供商那里购买托管服务，然后转卖给他们自己的客户。

云迁移(Cloud Migration)是将公司的全部或部分数据、应用系统和服务从公司内部站点转移到云端的过程。云迁移完成后，这些信息由互联网上的云端服务按需提供。

云操作系统(Cloud OS)是常用于替代 PaaS 模型的用语，表示与云计算的结合关系。

云可移植性(Cloud Portability)是在一个云服务提供商和另一个云服务提供商之间(或传统系统和云环境之间)迁移应用系统和相关数据的能力。

云服务提供商(Cloud Provider)是通过公共网络(通常是互联网)向云客户提供存储或软件解决方案的服务提供商。云服务提供商决定了所使用的技术和运维流程。

云服务代理商(Cloud Services Broker，CSB)通常是第三方的实体或公司，通过与多个云服务提供商之间的商业关系，向多个云客户提供扩展的或增强的基于云服务的价值。CSB 往往充当云客户和云服务提供商之间的中介，为每个云客户选择最佳云服务提供商并提供相关服务的持续监测。

云存储(Cloud Storage)在云端存储数据。一家公司的数据以可访问的形式存储在云上，而云由多个分布并连接的资源组成。

云测试(Cloud Testing)指负载和性能测试(特别是访问服务的能力)是在云服务提供商提供的应用系统和服务上进行的，以确保在多种条件下实现最佳性能和可伸缩性。

社区云(Community Cloud)是一个模型，其云计算基础架构是为特定社区专门设计的。通常情况下，社区的云用户和云客户有相同的考虑、业务使命和安全要求。

企业应用系统(Enterprise Application)是指为企业所用，帮助组织解决企业问题的应用系统或软件。

Eucalyptus 是私有云使用的、开源的云计算和 IaaS 平台。

FIPS 140-2 是一个 NIST 文档，该文档列出经过认证的和不再使用的密码体制。

混合云(Hybrid Cloud)是一种混合了公有云、私有云和社区云多种模型元素的云计算解决方案。

基础架构即服务(IaaS)是云计算服务的三种主要类型之一，其他两种类型是软件即服务(SaaS)和平台即服务(PaaS)。IaaS模型仅提供硬件和基础管理，由云客户负责操作系统和其他应用软件。

托管服务提供商(Managed Service Provider)是由云客户指定技术和运维流程的 IT 服务，外部合作伙伴根据合同执行管理和运维支持。

多租户(Multi-Tenant)是指多个云客户使用相同的云环境(通常是虚拟化环境中的同一主机)。

NIST 800-53 指导文件的主要目标是确保美国联邦政府信息管理系统中的所有信息满足适当的安全要求和控制项。

PaaS是一种让客户通过互联网从云服务提供商那里租用硬件、操作系统、存储和网络能力的方式。PaaS 是云计算服务的三种主要类型之一，其他两种类型是 SaaS 和 IaaS。

私有云(Private Cloud)用于描述在组织内实施的云计算平台。私有云的设计目的是提供与公有云系统相同的功能和益处，同时消除对云计算模型的一些异议。这些异议包括，对企业或云客户数据的控制、对安全的担忧以及与法律法规的合规或符合合同协议相关的问题。

SaaS 是一种软件交付方法。SaaS 模型提供了通过基于 Web 的服务远程访问软件及其功能的方式。因为 SaaS 模型的定价基于每月费用，SaaS 允许组织以比购买许可授权更低的成本访问业务功能。SaaS 模型是云计算服务的三种主要类型之一，其他两种类型是 PaaS 和 IaaS。

可信云计算(TCI)参考模型是云服务提供商的指南。TCI 允许云服务提供商创建一个完整的体系结构(包括数据中心的物理设施、网络的逻辑布局和需要使用这两者的流程)。云客户可以放心和自信地购买和使用云服务。要了解更多信息，请访问 https://cloudsecurityalliance.org/wp-content/uploads/2011/10/TCI-Reference-Architecture-v1.1.pdf。

供应商绑定(Vendor Lock-in)指云客户由于技术性或非技术性限制而无法迁移或转移到另一个云服务提供商的情况。

供应商锁定(Vendor Lock-out)指因为云服务提供商破产或以其他方式离开市场，从而导致云客户无法恢复或访问自己数据的情况。

虚拟化(Virtualization)指创建某项事物的虚拟(逻辑的或物理的)实例，包括虚拟计算机硬件平台、操作系统、存储设备和计算机网络资源。计算机硬件虚拟化是提高整体效率的一种方法，涉及在硬件中为虚拟化提供支持的 CPU，以及其他有助于改善客户环境性能的硬件组件。

成功的 CCSP 应试者应该熟悉这些术语。本书将逐一详细讨论这些术语。

基础知识回顾

同样重要的是要记住在本行业中使用的所有安全基本要素。例如，在 CBK、考试和本书中被广泛提及的 CIA 三元组。

- 机密性(Confidentiality)：保护信息免受未经授权的访问/传播。
- 完整性(Integrity)：确保信息不被未经授权地篡改。
- 可用性(Availability)：确保授权用户可在允许的情况下访问信息。

1.5　云计算的基本概念

云计算的一些概念在整个云计算主题的讨论中随处可见。这里对这些概念作一下

介绍。这些概念包含在本书的各种讨论中，CCSP 应试者应该熟悉这些概念。

1.5.1　敏感数据

每个组织都有自己的风险偏好(Risk Appetite)和保密意愿。无论每个云客户对其数据的敏感性做出何种决策，云服务提供商都必须提供某种方法，让云客户根据数据的敏感程度对数据进行分类(Categorization)和分级(Classification)，并提供足够的控制措施来确保这些类别的数据分别得到相应的保护。

1.5.2　虚拟化技术

虚拟化(Virtualization)技术使云计算服务成为经济上可行的业务模式。云服务提供商可为各种数量级的云客户和云用户提供服务，允许这些云客户和云用户购买和部署任意数量的主机，从而不会浪费云服务提供商的能力或导致资源闲置。

在虚拟化环境中，云用户可登录到云端网络，并启动一个台式计算机的虚拟实例。对于云用户来说，虚拟机(Virtual Machine，VM)和传统计算机之间没有明显的区别。然而，从云服务提供商的角度看，虚拟机给予云用户的只是一个软件，而不是一个真实存在的、由云用户专门操作的独占硬件。实际上，在云计算空间的单个主机上，同时运行的虚拟机可能有几个甚至几十个。当云用户注销或关闭虚拟机时，云端网络将捕获云用户虚拟机的快照(Snapshot)，将这个快照保存为单个文件，并存储在云端的某个位置，当云用户再次提出访问请求时，虚拟机可完全恢复到云用户之前离开时的情景。

通过这种方式，云服务提供商可为任何数量的云客户和云用户提供服务，而不需要为每个新的云用户购买新的硬件设备。规模经济允许云服务提供商以更低的成本和更好的服务，提供云用户期望的类似于传统网络的基本 IT 服务。

市场上有许多虚拟化产品供应商，例如 VMware 公司和 Microsoft 公司。虚拟化技术可使用多种实现方式。两种基本虚拟化类型是类型 1 和类型 2。

1.5.3　加密技术

作为信息安全专家，你应该已经非常熟悉加密技术的基本概念和工具了。在云计算技术服务方面，加密技术起到保护和增强云计算技术安全性的巨大效用，同时也带来了额外的问题与挑战。

由于组织的云数据处于由组织以外的其他人员控制和操作的环境中，因此加密提供了一定程度的安全保证。未经授权人员将不能在访问组织数据时理解这些数据的真实含义。组织可在数据到达云端之前对其进行加密，且只在必要时对其进行解密。

另一个与云操作相关的问题是远程访问。与其他远程访问一样，不管风险多大，

远程访问总面临着数据拦截、窃听和中间人攻击的风险。加密技术可在一定程度上缓解这些威胁，从而减轻云客户对这类问题的忧虑；如果数据在传输中被加密，即使数据被截获，也很难被未授权人员理解。

1.5.4　合规与持续审计

云计算服务为合规和持续审计(On-going Audit)带来了特定的挑战和机会。

从合规的角度看，云服务提供商能为特定监管体系下的组织提供整体合规解决方案。例如，云服务提供商可能有一个现存的、已知的、经过测试的整体解决方案，该方案符合 PCI、HIPAA 或 GLBA 的控制集合和步骤概要。由于试图将合规的难度和所花费的精力从云客户组织转移到云服务提供商一方，这一服务对于潜在云客户非常具有吸引力。

与此相反，持续审计变得更困难。云服务提供商极不愿意开放物理访问的许可，这包括任何对云服务提供商设施的访问或分享网络部署图以及安全控制列表。维护这些内容的机密性可增强云服务提供商的整体安全水平。然而，这些却是审计工作的基本要素。此外，正如接下来介绍的，很难确定某个组织的数据在某一时刻位于云环境中的哪一物理位置，或者哪些设备承载了哪个云客户的数据，因此，持续审计变得更困难。审计需要云服务提供商的合作，而云服务提供商迄今为止，不同意提供达到这一审计目的所需的准入要求。相反，云服务提供商通常会提供他们自己的审计成功的声明(通常以 SSAE SOC 3 报告的形式提供)。任何考虑向云迁移的组织都应该与监督他们的监管代理机构进行协商，确定这一有限的审计能力是否足以让监管机构满意。

1.5.5　云服务提供商的合同

云服务提供商和云客户之间的业务安排通常会采取合同(Contract)和服务水平协议(Service Level Agreement，SLA)的形式。合同将详细说明协议的所有条款：每一个参与方负责的服务内容、将采取何种服务形式以及出现问题将如何解决，等等。SLA 将在一定的时间范围内，为这些服务设置特定的、量化的目标和相应的配置。

例如，合同可能规定：“云服务提供商将确保云客户能持续、不间断地访问自己的数据存储资源”。然后，SLA 将明确定义“持续、不间断地访问”意味着“对数据存储的连接中断在每个自然月不超过三秒”。该合同还将说明当云服务提供商在给定时间段内未能满足 SLA 时所受的惩罚(通常是财务方面的)：“若云服务提供商未达到约定的服务水平，客户的费用将在下一个自然月予以免除。”

上面的简单示例演示了合同、SLA、云服务提供商和云客户之间的关系。本书将根据这里解释的关系，不断引用合同和 SLA。

1.6　小结

本章探讨业务需求、云计算的定义、云计算的角色和职责以及云计算的基本概念。本章是概述性的，后续章节将更详细地探讨这些主题。

1.7　考试要点

理解业务需求。始终牢记，包括安全和风险决策在内的所有管理决策都由业务需求驱动。在做出这些决定前，应慎重考虑安全和风险，但安全和风险不得优先于组织的业务需求和运营要求。

理解云计算术语和定义。务必清楚地理解本章中介绍的定义。CCSP 考试内容大多集中在术语和定义上。

能够描述云服务模型。至关重要的是，需要理解三种云服务模型(IaaS、PaaS 和 SaaS)之间的差异，以及与每种云服务模型相关的不同特性。

理解云部署模型。理解四种云部署模型(公有云、私有云、社区云和混合云模型)的特性以及它们之间的差异也很重要。

熟悉云计算的角色和相关责任。确保理解每个角色的不同和每个角色的职责。后续章节将更详细地探讨这些角色。

1.8　书面实验题

1. 访问CSA网站 https://cloudsecurityalliance.org/education/white-papers-and-educational- material/courseware/，观看题为“云计算入门”的视频。完成后花一些时间浏览该网站。
2. 写下你能想到可能促使组织考虑向云迁移的三个合法的业务驱动因素。
3. 列出三种云服务模型以及各自的优缺点。

1.9　复习题

可以在附录 A 中找到答案。

1. 以下哪一个不是通用的云服务模型？

   A. 软件即服务　　B. 程序即服务

   C. 基础架构即服务　　D. 平台即服务

2. 以下这些技术使云服务变得可行，除了：
   A. 虚拟化　　B. 广泛的网络连接
   C. 加密连接　　D. 智能集线器
3. 云计算供应商通过以下哪个方面承担合同义务？
   A. SLA　　B. 法规
   C. 法律　　D. 纪律
4. _____推动了安全相关的决策。
   A. 客户服务响应　　B. 调查
   C. 业务需求　　D. 公众舆论
5. 如果云客户无法访问云服务提供商，这会影响 CIA 三元组的哪一部分？
   A. 完整性　　B. 授权
   C. 机密性　　D. 可用性
6. 云访问安全代理商(CASB)可提供以下所有服务，除了：
   A. 单点登录　　B. 业务连续性/灾难恢复/运营连续性
   C. IAM　　D. 密钥托管
7. 加密可用于云计算的以下方面，除了：
   A. 存储　　B. 远程访问
   C. 安全会话　　D. 磁条卡
8. 以下所有这些都是一个组织可能考虑云迁移的原因，除了：
   A. 减少人员费用　　B. 消除风险
   C. 减少业务费用　　D. 提高效率
9. 普遍接受的云计算定义包括下列所有特点，除了：
   A. 按需自助服务　　B. 协商的备份需求
   C. 资源池　　D. 计量的服务
10. 以下所有情况都可能导致供应商绑定，除了：
   A. 不利的合同　　B. 合规
   C. 专有数据格式　　D. 不足的带宽
11. 云服务提供商停业导致云客户无法恢复数据的风险被称为：
   A. 供应商关闭　　B. 供应商锁定(Vendor Lock-Out)
   C. 供应商绑定(Vendor Lock-In)　　D. 供货路径
12. 所有这些都是云计算的特点，除了：
   A. 广泛的网络接入　　B. 反向收费配置
   C. 快速扩展　　D. 按需自助服务
13. 当云客户将个人身份信息(PII)上传到云服务提供商时，谁最终会为 PII 的安全性负责？
   A. 云服务提供商　　B. 监管机构
   C. 云客户　　D. 作为 PII 主体的个人

14. 我们使用下列哪一个来确定组织的关键路径、过程和资产？

A. 业务需求　　B. 业务影响分析(BIA)

C. RMF 模型　　D. CIA 三元组

15. 哪种云部署模型中，组织对硬件和基础架构拥有所有权，这种云仅被组织成员使用？

A. 私有云　　B. 公有云

C. 混合云　　D. 动机

16. 哪种云部署模型的云由云服务提供商所有，并提供给想要订购的任何人？

A. 私有云　　B. 公有云

C. 混合云　　D. 潜在的

17. 以共同拥有资产为特征的云部署模型被称为：

A. 私有云　　B. 公有云

C. 混合云　　D. 社区云

18. 如果云客户想要一个安全、隔离的沙箱以进行软件开发和测试，那么哪种云服务模型可能是最好的？

A. IaaS　　B. PaaS

C. SaaS　　D. 混合云

19. 如果云客户想要一个可完全操作的环境，需要很少的维护或管理，那么哪种云服务模型可能是最好的？

A. IaaS　　B. PaaS

C. SaaS　　D. 混合云

20. 如果云客户想要一个裸机环境，以业务连续性和灾难恢复为目的，在其中复制自己的公司环境，哪个云服务模型可能是最好的？

A. IaaS　　B. PaaS

C. SaaS　　D. 混合云