安全技术经典译丛

云安全 CCSP 认证官方指南

(第 2 版)

[美] 本•马里索乌(Ben Malisow) 著

(ISC)^2 北京分会 译

清华大学出版社

北 京

北京市版权局著作权合同登记号　图字：01-2020-6238
Ben Malisow
CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide, Second Edition
EISBN：978-1-119-60337-5

图书在版编目(CIP)数据

云安全CCSP认证官方指南：第2版 / (美)本 • 马里索乌(Ben Malisow) 著；(ISC)^{2}北京分会译. —北京：清华大学出版社，2021.7
(安全技术经典译丛)
书名原文：CCSP (ISC)^2 Certified Cloud Security Professional Official Study Guide, Second Edition
ISBN 978-7-302-58474-2

Ⅰ. ①云… Ⅱ. ①本… ②I… 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(2021)第 113743 号

责任编辑：王　军
装帧设计：孔祥峰
责任校对：成凤进
责任印制：刘海龙

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：三河市科茂嘉荣印务有限公司
经　　销：全国新华书店
开　　本：170mm×240mm　　**印　　张**：18.25　　**字　　数**：389 千字
版　　次：2021 年 7 月第 1 版　　**印　　次**：2021 年 7 月第 1 次印刷
定　　价：98.00 元

产品编号：087769-01

译 者 序

自从 Google 首席执行官埃里克•施密特在 2006 年提出“云计算”概念以来，云计算技术经历十多年的迅猛发展，取得了长足进步。随着大数据、云计算、物联网等技术的日益成熟，推动互联网向各个领域拓展，各大厂商也不断推出各种云计算的产品和服务。

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”。云计算是信息时代的一种创新；具有很强的扩展性和需要性，使用者通过网络可以获取无限的资源，不受时间和空间的限制。云计算利用虚拟化技术可以实现动态扩展，根据使用者的实际需求，灵活地配备相应的资源和计算能力，应用资源也可以通过部署在不同的虚拟化资源上，来提高云计算的操作水平。

新的技术也带来新挑战。在云计算的架构下，云计算开放网络和业务共享场景更加复杂多变，安全性方面的挑战更加严峻，一些新型的安全问题变得比较突出，如多个虚拟机租户间并行业务的安全运行，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。

紧随云计算、云存储之后，云安全顺势而生。云安全融合了并行处理、网络计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中的木马、恶意程序等最新信息，实时进行采集、分析和处理。

作为国际性安全行业观察者，$(ISC)^2$ 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础知识，并具有一定的工作经验。本书不介绍基础内容，但这些在考试中会出现。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与$(ISC)^2$ 北京分会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，非常感谢$(ISC)^2$ 北京分会主席卢佐华先生，以及张士莹、徐一、张云鹏、王林海、王伏彧、林进峰、李松恬、杜翔宇、白玉强等诸多分会成员对本书翻译的贡献。

衷心感谢本书英文版的作者和编辑们，是他们的支持和授权，才使这本书的中文版本得以顺利出版，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成就一番辉煌事业！

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、Katie Wisor 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。

作 者 简 介

Ben Malisow，持有 CISSP、CISM、CCSP、SSCP 和 Security+认证，担任 CISSP、CCSP 和 SSCP 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–梅隆大学的 CERT/SEI、UTSA、南内华达学院以及拉斯维加斯公立学校 6 到 12 年级的学生。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

Aaron Kraus 从业之初担任美国联邦政府客户的安全审计员，此后从事医疗和金融服务的安全风险管理工作，这为他提供了更多旅行、探险和品尝世界各地美食的机会。目前，Aaron 在美国旧金山的一家网络风险保险初创公司工作，业余爱好主要有烹饪、调制鸡尾酒和摄影。

前　言

CCSP (Certified Cloud Security Professional，云安全认证专家)认证满足了不断增长的云安全专业人员的需求。获得这个资格证书并不容易，考试极其困难，认证时间长、环节多。

本书为云安全专业人员参加并通过 CCSP 考试奠定了坚实的基础。对于计划参加考试并获得证书的读者来说，有一点需要再三强调：不能期望仅学习这一本书就通过考试。请参阅前言末尾的“推荐读物”。

$(ISC)^2$

CCSP 考试由 $(ISC)^2$ (International Information Systems Security Certification Consortium，国际信息系统安全认证联盟)管理。$(ISC)^2$ 是一个全球性非营利组织，有以下 4 个主要任务目标：

- 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、HCISPP 以及本书描述的 CCSP 认证。这些认证旨在验证所有行业的 IT 安全专业人员的知识和技能。通过访问 www.isc2.org，可以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 6 个知识域的内容，具体如下。

知识域 1：云概念、架构和设计

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：云安全运营

知识域 6：法律、风险与合规

这些知识域涵盖了与云相关的所有安全范围。认证中的所有内容都与厂商和产品无关。每个知识域都提供 CCSP 认证专业人士应该知道的主题及子主题列表。

关于知识域、经验要求、考试程序和考试域权重的详细清单，可以在 CCSP 认证考试大纲中找到: https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CCSP-Exam-Outline.ashx。

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：

- 至少累积 5 年全职带薪的信息技术工作经验，其中 3 年必须在信息安全领域工作，1 年必须在 CCSP 考试 6 个知识域中之一的领域工作。
- 获得云安全联盟(CSA)的 CCSK 证书，可替代 CCSP 考试 6 个知识域之一的领域的一年工作经验。
- 获得 CISSP 证书，可替代全部 CCSP 认证对工作经验的要求。

不符合这些要求的考生仍可参加 CCSP 考试并申请(ISC)^2 的准会员资格，准会员有 6 年的时间(从通过考试起)来满足剩余的经验要求。

(ISC)^2 认证会员必须遵守(ISC)^2 正式道德规范，该规范可以在 www.isc2.org/ethics 站点找到。

CCSP 考试概述

CCSP 考试通常包括 125 道选择题，涵盖 CCSP CBK 的 6 个领域，考生必须达到满分的 70%的分数或更高的分数才能通过。

CCSP 考试时间是 3 小时。其中有 25 道题仅用于研究目的，不计分数。尽全力回答每一道问题。因为我们不知道哪些问题计分，哪些不计。不答记零分，答错不扣分；即使是猜测，也要答完所有考题。

CCSP 考题类型

CCSP 考试中的大多数问题是单项选择题，每题有 4 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. 为了提供更高级别的保护和隔离，将敏感的操作信息放在远离生产环境的数据库中称为_____。

A. 随机化　　B. 弹性

C. 混淆　　D. 令牌化

CCSP 应试者需要选择正确或最佳答案。有时答案很明显，比较困难的时候是在两个好答案之间进行区分并选出最好的。留意对一般、特定、通用、超集和子集答案的选择。还有些情况是，没有一个答案看上去是正确的。这时，CCSP 应试者需要选择错误程度最小的答案。还有一些问题是基于理论场景的，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 D，令牌化。在令牌化管理中，敏感信息放在远离生产环境的数据库中，而令牌(表示存储的敏感信息)则存储在生产环境的数据库中。为了选择正确的答案，读者必须了解令牌化的工作原理，以及如何使用该方法将敏感数据与生产环境隔离开来；这个问题中没有提到令牌或令牌化，因此需要复杂的思考。更简单的一个答案是“数据隔离”，但没有这个选择项。这道题不容易答对。

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

本书建议应试者为 CCSP 考试，至少安排 30 天的强化学习。这里整理了一份备考技巧清单，希望对考生有所帮助。

- 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，与其他考生分享见解和观点。
- 回答所有复习题并参加模拟考试(Sybex 网站为本书提供的)。
- 完成每章的书面实验题。
- 在学习下一部分之前，请务必复习前一天的内容，以确保信息的掌握。
- 学习时注意适度休息，但要一直持续学习。
- 制订学习计划。
- 复习$(ISC)^2$ 考试大纲。

参加考试的建议

以下是一些考试技巧和通用指南。

- 先做简单题。考生可以标记所有不确定的题目，并在完成全部题目后重新检查一遍。
- 首先排除错误答案。

- 注意题目表达中的双重否定。
- 仔细读题，确保充分理解题意。
- 慢慢来，别着急。匆忙会导致考试焦虑和注意力不集中。
- 如果需要，可以上个厕所，休息一下，但是时间要短。考生需要保持注意力。
- 遵守考试中心的所有规程。即使考生以前参加过 Pearson Vue 中心的考试，有些考试的要求也略有不同。

管理好时间。考生有 3 小时回答 125 道考题，平均每道题不到 90 秒，对于大多数题目，答题时间是充足的。

确保考试前一晚有充足的睡眠。考生应带上可能需要的食物和饮料，在考试的时候要把它们存放起来。此外，记得带上需要服用的药物，并提醒工作人员任何可能会影响考生考试进行的健康情况，如糖尿病或心脏病。自己的健康比任何考试或认证都重要。

不能戴手表进入考场。计算机屏幕和考场内都有计时器。考生必须清空口袋进入考场，只能带储物柜钥匙和身份证件。

前往考试中心时，考生必须携带至少一张带照片并有签名的身份证件(如驾照或护照)，并且还必须携带至少一份带签名的身份证件。至少提前 30 分钟到达考场，以确保考试所需物品俱全。请携带考试中心寄来的包含考生身份证明信息的报名表。

完成认证过程

一旦 CCSP 应试者成功通过了 CCSP 考试，在获得新的证书之前还有几件事要做。首先，$(ISC)^2$ 考试成绩会自动传送。在离开考试中心时，CCSP 应试者会收到打印的考试结果说明。其中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其他$(ISC)^2$ 认证(如 CISSP)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 CCSP 应试者会在 3 个月内收到官方认证通知。获得完全认证后，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。

内容组织结构

本书以足够的深度涵盖了 CCSP CBK 的所有 6 个领域，为应试者理解这些考试内容提供了基本介绍。本书正文由 11 章组成，内容安排如下。

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)

显然本书没有按照知识域或官方考试大纲的顺序来安排章节。而是以叙事风格介绍内容，以线性方式表达概念。

每一章都包括辅助应试者学习的部分，和测试应试者对本章知识掌握程度的练习。这里建议应试者先阅读第 1 章，以便在阅读其他章节之前更好地了解主题。

注意：想要了解每章所涉及的更详细的知识域主题，请参阅目录和章节介绍。

特色小节

本学习指南通过一些特色小节，帮助应试者准备 CCSP 考试以及考试以外的实际工作。

真实世界场景：本书提供了一些真实世界场景，通过了解某些解决方案在现实世界的什么地方和什么情况下有效(或无效)以及原因，来帮助 CCSP 应试者进一步透彻理解相关信息。

小结：小结是对本章重要观点的快速概述。

考试要点：突出了一些可能在考试中以某种形式出现的主题。虽然作者并不确切知道具体考试将包括哪些内容，这部分强调了重要的概念，这对理解 CBK 和 CCSP 考试的测试规范是至关重要的。

书面实验题：每章提供书面实验题，将本章提出的各种主题和概念结合在一起。虽然这些内容是为大学(学院)的课堂使用而设计，但也可以帮助应试者理解和阐明课堂以外的内容。书面实验题的答案在附录 A。

复习题：每章提供练习题，用来测试应试者对本章讨论基本思想的掌握程度。应试者学完每一章后，回答问题；如果不能正确回答某些题目，则表明需要花更多时间研究相应的主题。复习题的答案在附录 B。

学习建议(注：译者补充)

本学习指南通过很多特色设置帮助 CCSP 应试者完成学习。在每章开头列出了该章涵盖的 CCSP 知识域主题，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。这里给出一些建议，帮助 CCSP 应试者取得更圆满的学习效果：

- 在开始阅读本书前完成评估测试。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。

请扫描封底二维码获取本书配套的在线学习工具。

推荐读物

为了更好地准备考试，除了学习本书之外，考生一定要复习其他资料。作者建议你至少参考以下资料。

Cloud Security Alliance, Security Guidance v4.0:

https://cloudsecurityalliance.org/research/guidance

OWASP, Top Ten:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

注意：本书英文版出版时，2017 年版本的 OWASP 十大威胁是最新版本，但版本差异不大，理解任何版本的概念将有助于研究目的。

NIST SP 800-53:

https://nvd.nist.gov/800-53

注意：本书英文版出版时，“NIST SP 800-53，R4”是最新版本，但是一个新的版本，预计很快就会推出。

NIST SP 800-37:
https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
The Uptime Institute, Tier Standard: Topology:
https://uptimeinstitute.com/resources/asset/tier-standard-topology
Cloud Security Alliance, Cloud Controls Matrix:
https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v1-0/
Cloud Security Alliance Consensus Assessments Initiative Questionnaire:
https://cloudsecurityalliance.org/artifacts/
consensus-assessments-initiative-questionnaire-v3-0-1/
Cloud Security Alliance STAR Level and Scheme Requirements:
https://cloudsecurityalliance.org/artifacts/star-level-and-schemerequirements
CCSP Official (ISC)^2 Practice Tests :
https://www.wiley.com/en-us/CCSP+Official+%28ISC%292+Practice+Testsp-9781119449225

评估测试

1. 企业或个人使用_____，可以通过存储服务提供商在互联网上存储数据和计算机文件，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，_____并非云客户的必然优势。

A. 不用维护许可证库　　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. 信息版权管理(IRM)　　B. 遮蔽

C. 位裂　　D. 消磁

4. _____是正确的 4 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. _____是一个特殊的数学代码，允许对硬件/软件进行加密，以及解密加密的消息。

A. PKI　　B. 加密密钥

C. 公钥-私钥　　D. 遮蔽

6. _____列出了 STRIDE 威胁模型的 6 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、拒绝服务和社交工程弹性

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. 描述保证特定发送者实际创建并向指定收件人发送具体信息，以及成功接收的术语是_____。

A. PKI　　B. DLP

C. 不可抵赖　　D. 位裂技术

8. 对于故意销毁用于加密数据的加密密钥的过程，正确的术语是_____。

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，他们使用身份提供者生成的令牌。

B. 依赖方是服务提供者，他们使用客户生成的令牌。

C. 依赖方是客户，他们使用身份提供者生成的令牌。

D. 依赖方是身份提供者，他们使用由服务提供商生成的令牌。

10. 使用唯一标识符号/地址替换敏感数据的过程是_____。

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. 将应用软件从执行它的底层操作系统中抽象出来的软件技术，是_____。

A. 分区　　B. 应用程序虚拟化

C. 分布式　　D. SaaS

13. _____代表美国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法律。

A. PCI　　B. GLBA

C. SOX　　D. HIPAA

14. _____可以安全地存储和管理加密密钥，并用于服务器、数据传输和日志文件。

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，TOSM)

15. 什么类型的云基础设施供公众开放使用，并由云提供商拥有、管理和运营?

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_____。

A. 数据库应用本身　　B. 使用数据库的应用中

C. 连接到卷的实例上　　D. 一个密钥管理系统中

17. 根据非数值类别或级别，采用一组方法、原则或规则来评估风险的评估类型是_____。

A. 定量评估　　B. 定性评估

C. 混合评估　　D. SOC 2

18. _____是 CSA CCM(云安全联盟云控制矩阵)的最佳描述。

A. 一套对云服务提供商的监管要求

B. 一套对云服务提供商的软件开发生命周期要求

C. 一个安全控制框架，提供与主要行业公认的安全标准、法规和控制框架之间的映射/交叉关系

D. 不同安全域中的云服务安全控制清单

19. 当双方发生冲突时，_____是决定审理争端管辖权的主要手段。

A. 侵权法　　B. 合同

C. 普通法　　D. 刑法

20. 选择新的数据中心基础设置时，_____是最重要的安全考虑因素。

A. 当地执法部门的响应时间　　B. 邻近竞争对手设施的位置

C. 飞机飞行路线　　D. 公共基础设施

21. 在云环境中清理电子记录时，_____始终是安全的。

A. 物理破坏　　B. 覆写

C. 加密　　D. 消磁

22._____不代表网络攻击。

A. 泛洪攻击　　B. 拒绝服务

C. Nmap 扫描　　D. 暴力破解

23._____利用了在 BIA(业务影响分析)中开发的信息。

A. 计算 ROI(投资回报率)　　B. 风险管理分析

C. 计算 TCO(总拥有成本)　　D. 确保资产收购

24. 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。_____是对该种托管服务模型的最佳描述。

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. _____是美国为控制金融机构处理个人隐私信息的方式而制定的联邦法律。

A. PCI

B. ISO/IEC

C. GLBA (Gramm-Leach-Bliley Act)

D. 消费者保护法(Consumer Protection Act)

26. 安全套接字层(SSL)在保护无线应用协议(WAP)中的典型功能是保护存在于_____的信息传输。

A. WAP 网关和无线终端设备之间　B. Web 服务器和 WAP 网关之间
C. 从 Web 服务器到无线终端设备　D. 无线设备和基站之间

27. _____是服务机构的审计标准。

A. SOC 1　B. SSAE 18
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，然后转售给自己客户的公司是_____。

A. 云程序员　B. 云经销商(broker)
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_____。

A. 服务器托管　B. 传统计算
C. 云计算　D. 内联网

30. 分析应用程序源代码和二进制代码，通过编码和设计条件查找安全漏洞的一组技术是_____。

A. 动态应用程序安全测试(DAST)　B. 静态应用程序安全测试(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数据(因为基础设施或设备受损)，则云备份具有支持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. A。在 IaaS 模型中，用户必须维护云环境中使用的操作系统和应用程序的许可证。在 PaaS 模型中，操作系统的许可是由云供应商管理的，而客户需要管理应用程序许可；在 SaaS 模型中，客户才不需要管理许可库。

3. A。信息版权管理(IRM)通常也被称为数字版权管理(DRM)，旨在关注安全性和加密，以防止未经授权的复制，并将内容分发仅限于授权人员(通常是购买者)。遮蔽需要隐藏特定用户视图中的特定字段或数据，以限制生产环境中的数据暴露。位裂是一种跨越多个地理边界隐藏信息的方法，消磁是一种从磁性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。联合云、互联网和外部云都不是云模型。

5. B。加密密钥是正确答案：用于加密和解密信息的密钥。加密密钥是支持基于硬件或基于软件加密的数学代码，用于对信息进行加密或解密，并由参与通信的各方保密。PKI 用于创建和分发数字证书。公钥-私钥是指非对称加密中使用的密钥对(该答案对问题来说过于具体；选项 B 更可取)。遮蔽需要隐藏特定用户视图中的特定字段或数据，以限制生产环境中的数据暴露。

6. A。首字母缩略词 STRIDE 中的字母分别代表身份欺骗、篡改、抵赖、信息泄露、拒绝服务和特权提升(或扩大)。其他选项只是对正确内容简单的混淆或弄错。

7. C。“不可抵赖”意味着事务的一方不能否认他们参与了该事务。

8. D。加密擦除的行为是指销毁用于加密数据的密钥，从而使数据很难恢复。

9. A。身份提供者维护身份并为已知用户生成令牌。依赖方(RP)是服务提供者，并使用令牌。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。应用程序虚拟化将应用程序从执行它的底层操作系统中抽象出来。SaaS 是云服务模型。分区是内存的一个区域，通常在驱动器上。分布式通常表示用于同一目的的多台机器。

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电脑上找到。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。很简单，就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应用本身的引导记录中。

17. B。定性评估是一组基于非数学类别或级别评估风险的方法或规则。使用数学分类或级别被称为定量评估。没有所谓的混合评估，SOC 2 是有关控制有效性的审计报告。

18. C。CCM 交叉引用了许多行业标准、法律和准则。

19. B。当事人之间的合同可以确立解决争端的管辖权；这是决定管辖权的首要因素(如果合同中没有明确规定，将使用其他方法)。侵权法是指民事责任诉讼。普通法是指有关婚姻的法律，而刑法是指违反州或联邦刑法。

20. D。在给出的所有选项中，D 是最重要的。任何数据中心设施都要靠近保障能力强的公共基础设施，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. C。所有其他选项都表示特定的网络攻击。Nmap 是一个相对无害的，用于网络映射的扫描工具。虽然它可以用于收集网络信息，作为开发攻击过程的一部分，但它本身不是攻击工具。

23. B。此外，BIA 收集对风险管理分析和进一步选择安全控制至关重要的资产评估信息。

24. C。这就是 SaaS(软件即服务)模型的定义。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(金融服务改革法案，Gramm-Leach-Bliley Act)针对美国金融和保险机构，要求他们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，它是无线终端设备和 Web 服务器。

27. B。SOC 1 和 SOC 2 都是基于 SSAE 18 标准的报告格式。SOC 1 报告财务报告的控制，SOC 2(类型 1 和 2)报告与安全或隐私相关的控制。

28. B。云经销商购买托管服务，然后转售。

29. C。云计算建立在网格计算模型的基础上，通过网格计算可以共享资源，而不是让本地设备完成所有计算和存储功能。

30. B。静态应用程序安全测试(SAST)用于在代码加载到内存并运行之前，审查源代码和二进制文件以检测问题。

目　录

第 1 章　架构概念……1
1.1　业务需求……3
1.1.1　现有状态……4
1.1.2　量化收益和机会成本……5
1.1.3　预期影响……7
1.2　云计算的演化、术语和模型……8
1.2.1　新技术、新选择……8
1.2.2　云计算服务模型……8
1.2.3　云部署模型……10
1.3　云计算中的角色和责任……12
1.4　云计算定义……12
1.5　云计算的基本概念……14
1.5.1　敏感数据……14
1.5.2　虚拟化技术……14
1.5.3　加密技术……14
1.5.4　审计与合规……15
1.5.5　云服务提供商的合同……15
1.6　相关的新兴技术……16
1.7　小结……17
1.8　考试要点……17
1.9　书面实验题……17
1.10　复习题……17

第 2 章　设计要求……21
2.1　业务需求分析……22
2.1.1　资产清单……22
2.1.2　资产评估……22
2.1.3　确定关键性……23
2.1.4　风险偏好……24
2.2　不同类型云的安全注意事项……26
2.2.1　IaaS 注意事项……26
2.2.2　PaaS 注意事项……27
2.2.3　SaaS 注意事项……27
2.2.4　一般注意事项……27
2.3　保护敏感数据的设计原则……28
2.3.1　设备加固……28
2.3.2　加密技术……29
2.3.3　分层防御……30
2.4　小结……30
2.5　考试要点……31
2.6　书面实验题……31
2.7　复习题……31

第 3 章　数据分级……35
3.1　数据资产清单与数据识别……37
3.1.1　数据所有权……37
3.1.2　云数据生命周期……38
3.1.3　数据识别方法……41
3.2　司法管辖权的要求……43
3.3　信息权限管理……44
3.3.1　知识产权的保护……44
3.3.2　IRM 工具特征……48
3.4　数据控制……49
3.4.1　数据保留……50
3.4.2　合法保留……51
3.4.3　数据审计……51

3.4.4 数据销毁/废弃 …… 53
3.5 小结 …… 54
3.6 考试要点 …… 54
3.7 书面实验题 …… 55
3.8 复习题 …… 55

第 4 章 云数据安全 …… 59
4.1 云数据生命周期 …… 61
4.1.1 创建 …… 61
4.1.2 存储 …… 62
4.1.3 使用 …… 62
4.1.4 共享 …… 63
4.1.5 归档 …… 64
4.1.6 销毁 …… 65
4.2 云存储架构 …… 65
4.2.1 卷存储：基于文件的存储和块存储 …… 65
4.2.2 基于对象的存储 …… 66
4.2.3 数据库 …… 66
4.2.4 内容分发网络 …… 66
4.3 云数据安全的基本策略 …… 66
4.3.1 加密技术 …… 67
4.3.2 遮蔽、混淆、匿名化和令牌化 …… 68
4.3.3 安全信息和事件管理 …… 71
4.3.4 出口的持续监测(DLP) …… 72
4.4 小结 …… 73
4.5 考试要点 …… 73
4.6 书面实验题 …… 73
4.7 复习题 …… 74

第 5 章 云端安全 …… 77
5.1 云平台风险和责任的共担 …… 78
5.2 基于部署模型的云计算风险 …… 80
5.2.1 私有云 …… 80
5.2.2 社区云 …… 81
5.2.3 公有云 …… 82
5.2.4 混合云 …… 85
5.3 云计算风险的服务模型 …… 85
5.3.1 IaaS …… 86
5.3.2 PaaS …… 86
5.3.3 SaaS …… 86
5.4 虚拟化 …… 87
5.4.1 威胁 …… 88
5.4.2 对策 …… 90
5.5 灾难恢复和业务连续性 …… 92
5.5.1 云特定的 BIA 关注点 …… 92
5.5.2 云客户/云服务提供商分担 BC/DR 责任 …… 93
5.6 小结 …… 95
5.7 考试要点 …… 96
5.8 书面实验题 …… 96
5.9 复习题 …… 96

第 6 章 云计算的责任 …… 101
6.1 管理服务的基础 …… 103
6.2 业务需求 …… 104
6.3 按服务类型分担职责 …… 109
6.3.1 IaaS …… 109
6.3.2 PaaS …… 109
6.3.3 SaaS …… 110
6.4 操作系统、中间件或应用程序的管理分配 …… 110
6.5 职责分担：数据访问 …… 112
6.5.1 云客户直接管理访问权限 …… 112
6.5.2 云服务提供商代表云客户管理访问权限 …… 113
6.5.3 第三方(CASB)代表客户管理访问权限 …… 113
6.6 无法进行物理访问 …… 113

6.6.1 审计……113
6.6.2 共享策略……116
6.6.3 共享的持续监测和测试……117
6.7 小结……118
6.8 考试要点……118
6.9 书面实验题……118
6.10 复习题……119

第 7 章 云应用安全……123
7.1 培训和意识宣贯……125
7.2 云安全软件开发生命周期……129
7.3 ISO/IEC 27034-1 安全应用程序开发标准……131
7.4 身份和访问管理……132
7.4.1 身份存储库和目录服务……133
7.4.2 单点登录……133
7.4.3 联合身份管理……133
7.4.4 联合验证标准……134
7.4.5 多因素身份验证……135
7.4.6 辅助安全设备……135
7.5 云应用架构……136
7.5.1 应用编程接口……136
7.5.2 租户隔离……137
7.5.3 密码学……137
7.5.4 沙箱技术……138
7.5.5 应用虚拟化……139
7.6 云应用保证与验证……139
7.6.1 威胁建模……139
7.6.2 服务质量……141
7.6.3 软件安全测试……141
7.6.4 已核准的 API……143
7.6.5 软件供应链管理(API 方面)……143
7.6.6 开源软件安全……144
7.6.7 应用编排……144
7.6.8 安全网络环境……145
7.7 小结……146
7.8 考试要点……146
7.9 书面实验题……146
7.10 复习题……147

第 8 章 运营要素……151
8.1 物理/逻辑运营……153
8.1.1 设施和冗余……154
8.1.2 虚拟化运营……162
8.1.3 存储运营……163
8.1.4 物理和逻辑隔离……166
8.1.5 应用程序测试方法……167
8.2 安全运营中心……168
8.2.1 持续监控……168
8.2.2 事件管理……168
8.3 小结……170
8.4 考试要点……170
8.5 书面实验题……170
8.6 复习题……170

第 9 章 运营管理……173
9.1 持续监测、容量以及维护……174
9.1.1 持续监测……174
9.1.2 维护……175
9.2 变更和配置管理……179
9.3 IT 服务管理和持续服务改进……183
9.4 业务连续性和灾难恢复……184
9.4.1 主要关注事项……184
9.4.2 运营连续性……185
9.4.3 BC/DR 计划……185
9.4.4 BC/DR 工具包……187
9.4.5 重新安置……188

9.4.6 供电……189
9.4.7 测试……190
9.5 小结……190
9.6 考试要点……191
9.7 书面实验题……191
9.8 复习题……191

第 10 章 法律与合规(第一部分)……195
10.1 云环境中的法律要求与独特风险……197
10.1.1 法律概念……197
10.1.2 美国法律……200
10.1.3 国际法……202
10.1.4 世界各地的法律、框架和标准……202
10.1.5 信息安全管理体系(ISMS)……208
10.1.6 法律、规章和标准之间的差异……209
10.2 云环境下个人及数据隐私的潜在问题……210
10.2.1 电子发现……210
10.2.2 取证要求……211
10.2.3 解决国际冲突……211
10.2.4 云计算取证的挑战……212
10.2.5 直接和间接标识……212
10.2.6 取证数据收集方法……213
10.3 理解审计流程、方法论及云环境所需的调整……213
10.3.1 虚拟化……214
10.3.2 审计范围……214
10.3.3 差距分析……214
10.3.4 限制审计范围声明……215
10.3.5 策略……215
10.3.6 不同类型的审计报告……216
10.3.7 审计师的独立性……216
10.3.8 AICPA 报告和标准……216
10.4 小结……218
10.5 考试要点……218
10.6 书面实验题……218
10.7 复习题……219

第 11 章 法律与合规(第二部分)……221
11.1 多样的地理位置和司法管辖权的影响……223
11.1.1 策略……224
11.1.2 云计算对企业风险管理的影响……227
11.1.3 管理风险的选择……227
11.1.4 风险管理框架……230
11.1.5 风险管理指标……231
11.1.6 合同和服务水平协议(SLA)……232
11.2 业务需求……234
11.3 云计算外包的合同设计与管理……234
11.4 确定合适的供应链和供应商管理流程……235
11.4.1 通用标准保证框架……235
11.4.2 CSA STAR……236
11.4.3 供应链风险……236
11.4.4 相关方的沟通管理……237
11.5 小结……238
11.6 考试要点……238
11.7 书面实验题……238
11.8 复习题……239

附录 A 书面实验题答案……241

附录 B 复习题答案……249

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：云概念、架构和设计
  - 1.1 理解云计算概念
    - 1.1.1 云计算定义
    - 1.1.2 云计算角色
    - 1.1.3 云计算的关键特征
    - 1.1.4 构建块技术
  - 1.2 描述云参考架构
    - 1.2.1 云计算活动
    - 1.2.2 云服务功能
    - 1.2.3 云服务类别
    - 1.2.4 云部署模型
    - 1.2.5 云共享方面的考虑
    - 1.2.6 相关技术的影响
  - 1.4 理解云计算安全的设计原则
    - 1.4.3 成本效益分析
    - 1.4.4 功能安全需求
- ✓ 知识域 4：云应用安全
  - 4.7 设计适当的标识和访问管理(IAM)解决方案
    - 4.7.5 云访问安全代理(CASB)
- ✓ 知识域 5：云安全运营
  - 5.4 实施操作控制和标准
    - 5.4.10 服务水平管理

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，而是面向云计算安全领域的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，目前已经拥有一定的行业经验，从事信息安全相关工作，并能深入透彻地了解计算机、安全、业务、风险和网络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 考试范围会覆盖这些基础的安全知识。如果 CCSP 应试者没有 CISSP 认证背景，最好先学习一些与 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(CBK)中有一些特定的术语和概念，可能是 CCSP 中所独有的观点和用法，与你在日常 IT 运营中所理解的有所不同。因此，本章只是作为指南，在帮助你学习 CBK 及其他知识时奠定基础。

云特征

云计算意味着很多知识内容，但是，以下这些特性已成为被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
- 快速弹性
- 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 对“云计算”的官方定义是：“云计算是一个模型，实现无处不在的、便捷的、可通过网络按需访问的、可共享的、可配置计算资源池(包括网络、服务器、存储、应用及服务)，这些资源可以快速地获取和释放，同时最小化管理开销或与云服务提供商的交互。”

上述特征也符合 ISO 17788 中对云计算的定义(www.iso.org/iso/catalogue_detail?csnumber=60544)。本书、CBK 和考试都会涉及这些内容。

广泛的网络接入意味着可以始终使用标准的方式访问服务。例如使用 Web 浏览器访问“软件即服务”(SaaS)应用程序，而无须考虑用户的位置、计算机操作系统或浏

览器等的选择。这通常是通过使用先进的路由技术、负载均衡器、多站点托管(Multisite Hosting)等技术实现的。

按需自助服务指的是这样一个模型：它允许客户自主扩展计算和/或存储，而不需要或很少需要提供商的介入或提前沟通。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。云提供商的资产投入可以大大超过任何单个客户自己所能提供的，并且可以根据需要分摊这些资源，这样资源就不会出现低效利用(这意味着投资浪费)或超额使用(这意味着服务水平降低)。这通常称为多租户环境，即多个客户共享相同的底层硬件、软件和网络设施。

快速弹性允许客户根据需要增加或缩小 IT 资源占用(用户数量、机器数量、存储大小等)，能满足运营需求的同时又不会产生过剩容量。在云环境中，这可以瞬间完成，而在传统环境中，资源的获取和部署(或释放旧资源)可能需要数周或数月。

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。

后续章节会更详细地介绍所有这些概念。

真实世界场景

网上购物

假想年底假日前零售行业销售旺季的需求。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，在线购物零售商可以在云端托管销售业务并从中受益匪浅。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，并对这期间的新增使用量以协商后的价格进行收费。当节日过后销售量下降时，零售商不需要还按较高的价格来支付费用。

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。

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多地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。

功能性需求(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。

非功能性需求(Non-functional Requirements)：尽管不是设备、流程或员工完成业务目标所需的、但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。这不是一个容易的决定，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
- 采访高级管理人员
- 调查客户需求
- 收集网络流量
- 盘点资产
- 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，必须对此进行详细分析。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，需要确定需要付出多少成本才能合规，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：资产可以是有形的或无形的。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(如软件代码、思想表达和业务方法论)常是无法触及的。

1.1.2　量化收益和机会成本

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。下面介绍其中的一些考虑因素。

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，该设备的容量可能被充分利用，更可能得不到充分利用(能力闲置)。如果容量被充分利用了，很可能会在某个时刻效率低下。例如当对该设备的能力需求稍微提升时，就可能使该设备超出负荷，无法满足突发的使用要求。如果设备没有得到充分使用，那么组织就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。

此外，从购买设备中可以实现的税收优惠必须在经营年限中随同该设备/资产的折旧而被计入。对于付费服务(比如云服务)，作为运营支出，整个支付(可能是每月或每季)都可以作为费用抵税。

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，组织不需要对这些资产支付额外的费用。由于云服务提供商所拥有的云容量足以分配给云客户，因此，组织总能从容应对需求的增长(甚至是急剧的、快速的、大量的需求)，而不会不知所措(这就是前面描述的快速弹性)。

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)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)。

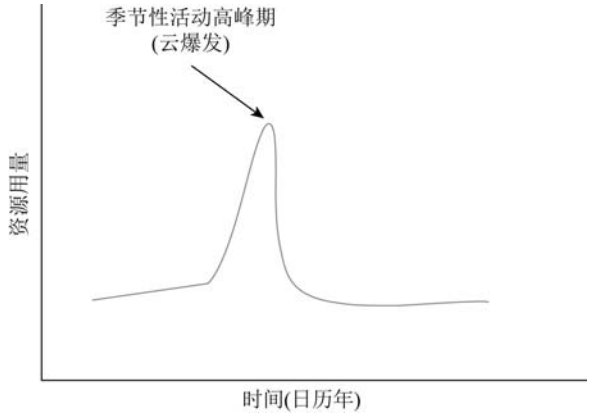

图 1.1　按需分配的弹性特性允许云客户定制资源的使用量

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，组织即便不会大量裁减高薪的 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。

在法律和经济等各个方面，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的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

所有这些收益都可以计算出具体的金额。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，以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：投资回报(ROI)是一个与成本效益度量相关的术语，也是一个用来描述盈利能力比率的术语，一般用净利润除以净资产来计算。

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、术语和模型

云计算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)：**组织可以与云供应商签订合同，而不是不断购买计算机、服务器、数据存储系统和其他资源，并在内部维护其基础设施。云提供商使用虚拟化灵活地将每个资源的所需使用量分配给组织，从而在保持收益的同时降低了成本。它还允许用户从不同的平台和位置访问他们的数据，增加了可移植性、可访问性和可用性。
- **简单化(Simplicity)：**正确的云实现方式应当允许用户无缝地使用服务，而不必频繁地与云服务提供商交互。
- **可伸缩性(Scalability)：**一般来说，对服务的增减比在非云环境中更容易、更快速、更划算。

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，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 供他们使用。

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 3 种通用模型。这 3 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 3 种模型。

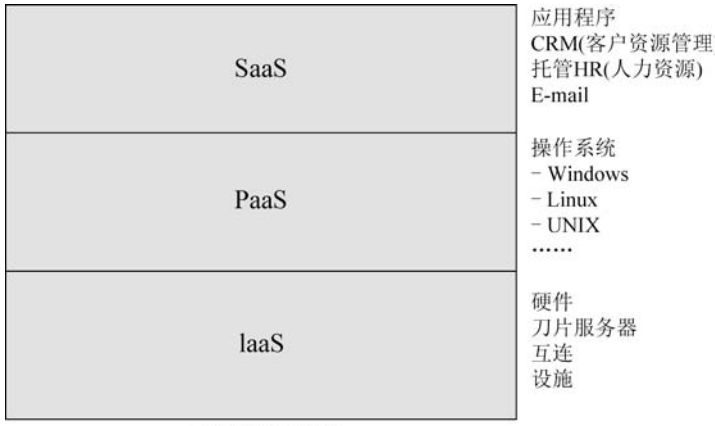

图 1.2　云计算服务模型

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 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 3 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。就客户支付给提供商的费用而言，它通常是最便宜的云服务选项。然而，客户将保留某些功能和需求，例如 IT 人员配置，这可能导致难于真正弄清投入的总体成本。

2. PaaS 模型

PaaS 模型包含 IaaS 模型中的所有内容，另外还加上了操作系统。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 还包括基于云的数据库引擎和服务，以及“大数据”模式的服务，如数据仓库和数据挖掘。供应商提供对后端引擎/功能的访问途径，而客户可以创建/安装各种应用程序/API 来访问后端。

3. SaaS 模型

SaaS 模型除包括前两个模型中列出的所有内容外，还额外添加了软件程序。云服务供应商也负责管理、打补丁和更新软件。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。

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)。公有云是多租户环境；多个客户将共享由提供商拥有和运营的基础资源。这意味着公有云中的客户使用的虚拟机可能实际上驻留在同一硬件上，而该硬件上可能托管着另一个由客户的直接竞争对手操控的虚拟机，而且客户无法知道还有其他哪些实体正在使用相同的资源。

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

2. 私有云

私有云(Private Cloud) 的典型特征是单个客户具有专用资源；其他客户不会共享底层资源(包括硬件，可能还有软件)。因此，私有云不是多租户环境。

私有云有诸多形式。私有云可以是由作为唯一客户的实体拥有和维护。换句话说，一个组织可能拥有并运营一个数据中心作为该组织用户的云环境。或者，私有云可以是由单个客户拥有的一整套资源(机架、刀片服务器、软件包)，但位于云提供商的数据中心并进行维护；云提供商可能为客户的资源提供物理安全性、一些基本管理服务和适当的公用设施(电源、Internet 连接)。这有时被称为“场地出租”(co-located)环境。

另一个私有云选项是让客户与云提供商签订协议，这样提供商就可以在公有云中为客户提供特定资源的独家使用权。基本上是提供商切割出整个数据中心的物理和逻辑部分，以免客户与任何其他客户共享该部分资源。显然，客户必须为这种类型的服务支付额外费用(高于多租户环境中公有云客户支付的费用)。

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。在这种类型的社区云中，底层技术(硬件、软件等)的责任权分散在社区的各个成员中。

社区云也可以由第三方代表社区的不同成员来提供。例如，云提供商提供一种 FedRAMP 云服务，仅供美国联邦政府客户使用。任何一家联邦机构都可以订购此云服务(例如农业部、卫生和公共服务部、内政部等)，它们都将使用严格为其专用的底层基础设施。任何非美国联邦机构的客户都不允许使用这个服务，因为非政府实体不属于这个特殊社区。云提供商拥有底层基础设施，但它仅供特定社区用户使用。

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)。

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。

云经纪人(Cloud Broker)是从云提供商那里购买托管服务的公司，将托管服务再转售给自己的客户。

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(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。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，这里不一一列举。

1.4 云计算定义

由于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，本节介绍其中的一些定义。

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(Cloud Application)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)使用计算、存储和网络资源，并具有快速弹性、计量服务、广泛的网络访问和合并资源的能力。

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。

成本效益分析将业务决策的潜在正面影响(如利润、效率、市场份额等)与潜在负面影响(如费用、对生产的不利影响、风险等)进行比较，并衡量两者是否等效，或者潜在正面影响是否大于潜在负面影响。这是业务决策，而不是安全决策，最好由经理或业务分析师做出。但是，为了做出明智的决定，有关各方必须拥有足够的见解和知识。在安全性方面，CCSP 应告知管理层与每个可选方案相关的特定风险和收益。

FIPS 140-2 是一个 NIST 文档，描述了被美国联邦政府使用的认证和加密系统的过程。

托管服务提供商(Managed Service Provider)是一种 IT 服务，其中客户指定技术和操作程序，由外部人员根据合同执行管理和操作支持。托管服务提供商可能会在该组织的业务位置或云中为该组织维护和管理数据中心/网络。

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措施。

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。

供应商锁定(Vendor Lock-out)，在由于技术或非技术限制而导致客户可能无法离开、迁移或转移到备用供应商的情况下，将发生供应商锁定。

供应商停业，当客户由于云提供商破产或以其他方式退出市场而无法恢复或访问自己的数据时，就会发生供应商停业。

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的篡改。
- 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。这里介绍这些概念。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，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，云用户可以访问合成计算机。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台甚至几十台。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注销或关闭时的情景。

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，提供云用户所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。这些将在 5.4 节“虚拟化”中进行描述。

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。

另一个与云运营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　审计与合规

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，将在第 6 章和第 10 章中进行讨论)。任何考虑向云迁移的组织都应该与监督它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。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 3 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 相关的新兴技术

有一些新兴和相关的技术值得一提。这些技术已在$(ISC)^2$ 考试大纲中明确列出，因此是 CCSP 候选人应该关注的技术。

- **机器学习和人工智能(AI)**：机器学习和 AI 均指程序和机器可以获取、处理、关联和解释信息，然后将其应用到各种功能中，而不需要用户或程序员直接输入的概念。各种各样的 IT 和云产品和服务声称具有机器学习或 AI 功能。其中包括防火墙、入侵检测/防御系统(IDS / IPS)、防病毒解决方案等。
- **区块链**：区块链是一种使用加密技术和算法传达价值的开放手段。它通常被称为“加密货币”。从根本上讲，这是一个交易账本，所有参与者都可以查看每一笔交易，因此，对过去交易的完整性产生负面影响变得极为困难。区块链可以被看作一种云技术，因为每个记录(“区块”)都以分布式或基于云的方式分布在所有参与者之间，而与位置、设备类型、权限等无关。
- **物联网(IoT)**：现在似乎每一种产品(如家用电器、相机、玩具、车辆等)都有可能包含网络连接。这些被统称为物联网(IoT)。这些设备的分布式特性(以及它们与网络的连接和放置)使它们具有一些云特征。物联网最显著的安全问题可能是没有适当安全措施的设备可以被破坏并用于攻击。
- **容器**：该术语指的是设备中存储空间的逻辑分段，以创建两个或更多无法直接接口的抽象区域。这通常可以在员工使用私人设备进行工作的自带设备(BYOD)环境中看到。容器区分了两个不同的分区，一个分区用于工作功能/数据，另一个分区用于个人功能/数据。这为雇主/数据所有者提供了额外的保证，即数据不会意外或偶然丢失或被盗。
- **量子计算**：这是一项新兴技术，可以使 IT 系统在二进制数学之外运行。量子计算可以使用亚原子特性(电子自旋、吸引力等)来提供指数级更大的计算，而不是使用电子的存在进行计算(电子以两种状态之一存在：存在或不存在)。这将大大提高机器执行计算/运算的能力。尽管在撰写本文时还不可被商业使用，但这种系统已开始超出理论阶段。
- **同态加密**：同态加密是一种理论现象，不必先解密就可以处理加密的材料。如果实现了这一点，则云客户可以将加密的数据上传到云，并且仍可使用该

数据，不必与云提供者共享加密密钥，也不必在过程中以其他方式接受解密。这将使云环境的使用对拥有高价值或敏感数据的客户更具吸引力。

1.7　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。

1.8　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 3 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 4 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。

1.9　书面实验题

在附录 A 中可以找到答案。

1. 进入 CSA 网站，并下载 https://cloudsecurityalliance.org/artifacts/security-guidance-v4/ 上的“针对云计算关键领域的安全指南”。完成后，花一些时间浏览该站点，自己查看文档。
2. 写下你能想到的可能促使组织考虑向云迁移的 3 个合法的业务驱动因素。
3. 列出 3 种云计算服务模型以及各自的优缺点。

1.10　复习题

在附录 B 中可以找到答案。

1. _____不是通用的云服务模型。
   A. 软件即服务(SaaS)　　B. 编程即服务(PaaS)
   C. 基础架构即服务(IaaS)　　D. 平台即服务(PaaS)
2. 以下这些技术使云服务变得可行，除了_____。
   A. 虚拟化　　B. 宽带连接
   C. 加密连接　　D. 智能集线器
3. 云计算供应商通过_____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_____。
   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(BC / DR / COOP)
   C. 身份和访问管理(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. 以下这些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. 被普遍接受的云计算定义包括下列特点，除了_____。
   A. 按需自助服务　　B. 不需要备份
   C. 资源池　　D. 计量服务
10. 玩家是 PlayStation Network 社区云的一部分。_____拥有游戏者家中的 PlayStation 控制台。
   A. 索尼
   B. 整个社区
   C. 制作当时玩家正在玩的游戏的公司
   D. 玩家

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. 以下是云计算的特点，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，_____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_____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. 主题云

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. 潜在云

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，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，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