网络空间安全丛书

# CCSP 云安全专家认证 All-in-One (第 2 版)

[美] 丹尼尔 • 卡特(Daniel Carter) 著
栾浩 陈英杰 张瑞恒 译
河北翎贺计算机信息技术有限公司 审

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：01-2021-7217
Daniel Carter
CCSP Certified Cloud Security Professional All-in-One Exam Guide, Second Edition
ISBN: 978-1-260-45692-9


**图书在版编目(CIP)数据**

CCSP云安全专家认证All-in-One：2版 / (美) 丹尼尔 • 卡特(Daniel Carter) 著；栾浩，陈英杰，张瑞恒译. —北京：清华大学出版社，2022.4
(网络空间安全丛书)
书名原文：CCSP Certified Cloud Security Professional All-in-One Exam Guide, Second Edition
ISBN 978-7-302-60334-4

Ⅰ. ①C… Ⅱ. ①丹… ②栾… ③陈… ④张… 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(2022)第 043517 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**：丛怀宇

**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：010-83470000 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**：大厂回族自治县彩虹印刷有限公司
**经 销**：全国新华书店
**开 本**：170mm×240mm **印 张**：16.5 **字 数**：455 千字
**版 次**：2022 年 5 月第 1 版 **印 次**：2022 年 5 月第 1 次印刷
**定 价**：98.00 元

产品编号：089304-01

# 译 者 序

我国“十四五”规划和2035年远景目标纲要提出加快推动数字产业化、推进产业数字化转型。这是把握世界科技革命和产业变革大趋势作出的战略部署，为我们打造数字经济新优势指明了方向。在数字经济正在成为经济发展核心驱动力的同时，云计算正在成为推动数字经济发展的重要驱动力。云计算的发展有利于加快软件和信息技术服务业发展，推动互联网、大数据、人工智能和实体经济深度融合。

近年来，云计算产业帮助企业提升业务敏捷性并降低成本，但也增加了安全攻击面。麦肯锡公司指出，40%的公司曾遭遇过基于云计算技术体系的数据泄露。2022年，预计每家组织都会遭遇至少一次云泄露。Ponemon Institute和IBM的另一项研究发现，云数据泄露给企业带来的平均损失高达361万美元。网络安全机构Sophos公司发布的《2020年云安全状况》调查报告显示，恶意软件、勒索软件、数据泄露、账户泄露以及加密劫持是最大的威胁。因此，在云计算推广的同时，安全性也不容小觑。政府、军队和广大企业需要培养具有云计算知识和安全能力的专家团队。

有鉴于此，清华大学出版社引进并主持翻译了《CCSP 云安全专家认证 All-in-One(第 2 版)》一书。本书基于最新的(ISC)²技术体系，涵盖六大知识领域：云概念、架构与设计，云数据安全，云平台与基础架构安全，云应用程序安全，云运营安全，法律、风险与合规。本书将CCSP考试所需的知识和对这些概念的运用场景结合在一起，是一本易于阅读、学习和参考的权威指南。本书自第1版出版以来就获得广泛好评，帮助广大云计算和信息安全从业人员全面、深入地理解云技术及云计算特有的安全问题和要求。

本书作者从事信息安全和教育工作 20 多年，是 $(ISC)^2$ 的认证讲师，讲授CISSP和CCSP课程。作者在撰写本书时借鉴了自己学习和通过考试的经验，以及多年讲授CISSP和CCSP课程的经验，帮助希望获取CCSP认证的人员备考。同时，本书也可作为从事云计算安全咨询和审计工作的人员的指导丛书。

本书的翻译历时年余全部完成。翻译中译者力求忠于原著，尽可能传达作者的原意。有近十名译者参与本书的翻译和校对工作，正是有了他们的辛勤付出才有了本书的出版。同时，感谢参与本书校对的网络安全专家，保证本书稿件内容表达的一致性和文字的流畅。感谢栾浩、姚凯、王向宇、陈英杰和吕丽在组稿、校对和通稿等工作所投入的大量时间和精力，保证了全书在技术上符合云计算安全工作实务，以及在内容表达上的准确性、一致性和连贯性。

同时感谢本书的审校单位河北翎贺计算机信息技术有限公司(简称“河北翎贺”)。河北翎贺基于多年积累的网络安全前沿技术和攻防实战方面的研究和实践经验，专业从事商用密码应用安全性评估、等级保护测评、风险评估、渗透测试、攻防演习、软件测试、安全运维、安全巡检、安全培训、安全加固和应急响应等一站式服务，客户涵盖政府、教育、医疗、金融、电力、通信以及能源等行业，河北翎贺始终致力于通过专业技术为客户提供更具实效的安全解决方案，用自身的专业能力和实际行动捍卫国家和企业的网络安全。在本书的译校过程中，河北翎贺的安全专家结合 CCSP 认证考试特点，投入了大量技术人员和时间支撑本书译校工作，保证了全书的质量。

最后，再次感谢清华大学出版社和王军等编辑的严格把关，悉心指导，正是有了他们的辛勤努力和付出，才有了本书中文译稿的出版发行。

本书横跨多个专业领域，内容涉猎广泛，术语体系复杂且难于辨析。译者在译校中难免有错误或不妥之处，恳请广大读者不吝指正。

# 译 者 简 介

**栾浩，**获得美国天普大学 IT 审计与网络安全专业理学硕士学位，持有 CISSP、CISA、CISP-A、TOGAF9、ISO27001LA 和 BS25999LA 等认证。现任 CTO 职务，负责金融科技研发、数据安全、云计算安全和信息科技审计和风控等工作。担任(ISC)²上海分会理事。栾浩先生担任本书的总技术负责人，并承担第 1 章、第 3~5 章的翻译工作，以及全书的校对和定稿工作。

**陈英杰，**获得北京交通大学海滨学院计算机科学与应用专业工学学士学位，持有国家互联网应急中心“网络安全能力认证(CCSC)”培训讲师、高级网络安全等级测评师等认证。现任河北翎贺计算机信息技术有限公司总经理，负责公司运营和安全技术管理工作。陈英杰女士承担全书的校对和定稿工作。

**姚凯，**获得中欧国际工商学院工商管理硕士学位，持有 CISSP、CCSP、CISA 和 CEH 等认证。现任 CIO 职务，负责 IT 战略规划、策略程序制定、IT 架构设计及应用部署、系统取证和应急响应、数据安全、灾难恢复演练及复盘等工作。姚凯先生承担本书前言、第 7 章的翻译工作，以及全书校对工作。姚凯先生为本书撰写了译者序。

**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 CISP、CISP-A 等认证。负责数据安全运营、安全工具研发、信息系统审计和软件研发安全等工作。王向宇先生承担本书第 6 章和附录的翻译工作，以及全书校对工作。

**吕丽，**获得吉林大学文秘专业文学学士学位，持有 CISSP、CISA、CISM 和 CISP-PTE 等证书。现任中银金融商务有限公司信息安全经理，负责信息科技风险管理、网络安全技术评估、信息安全体系制度管理、业务持续及灾难恢复体系管理、安全合规与审计等工作。吕丽女士承担全书术语校对工作，并担任本书项目经理，统筹各项事务。

**张瑞恒，**毕业于防灾科技学院计算机网络技术与信息处理专业，持有 CISSP、CISA 和 Prince2 等认证。负责 IT 内控、云计算安全运营企业 SOC 建设以及数据安全等工作。张瑞恒先生担任本书的云计算运营与技术顾问。

**徐坦，**获得河北科技大学理工学院网络工程专业工学学士学位，持有 CISP 等认证。现任安全渗透测试工程师职务，负责数据安全渗透测试、安全工具研发和企业安全攻防等工作。徐坦先生承担本书部分章节的校对工作。

**李浩轩，**获得河北科技大学理工学院网络工程专业工学学士学位，持有 CISP 等认证。现任安全渗透测试工程师职务，负责安全工具研发、应用安全检测、异常流量分析、攻击事件研判和网络攻击溯源等工作。李浩轩先生承担本书部分章节的校对工作。

**陈阳，**获得哈尔滨工程大学计算机软件工程硕士学位，持有 CISSP、CISA 等认证，现任高级技术经理职务，负责信息安全管理、信息风险管理、应急与灾备管理、事件管理、信息科技监管合规等工作。陈阳女士承担本书第 2 章翻译工作以及部分章节的校对工作。

**任寅，**毕业于河北工业大学计算机科学与技术专业，持有注册信息安全讲师(CISI)、国家互联网应急中心“网络安全能力认证(CCSC)”讲师等认证。现任河北翎贺计算机信息技术有限公司技术经理职务，负责网络安全等级测评、风险评估、商用密码应用安全性评估、信息安全审计等工作。任寅女士承担本书部分章节的校对工作。

**沈鹏，**毕业于西北工业大学网络工程专业，持有 CISP-PTE、国家互联网应急中心 CCSC 讲师等认证。现任河北翎贺计算机信息技术有限公司攻防实验室负责人职务，负责网络安全攻防对抗、溯源取证、商用密码应用安全性评估等工作。沈鹏先生承担本书部分章节的校对工作。

**任佩，**获得北京工业大学软件工程专业硕士学位，持有 CISP、信息安全等级测评师证书(高级)、信息系统项目管理师(高级)等认证。现任职于中国电科集团第十五研究所中电科认证测评中心网络安全测评部主管，负责网络安全等级测评、风险评估、商用密码应用安全性评估、信息安全审计等工作。任佩女士承担本书部分章节校对工作。

**李雅欣，**获得中南财经政法大学信息安全专业工学学士学位。现任解决方案工程师职务，负责数据安全产品方案及内容输出、安全工具产品说明和企业数据安全业务模型设计等工作。李雅欣女士承担本书部分章节的校对工作。

**刘波，**毕业于西北工业大学计算机科学与技术专业，持有 CISP、网络安全等级测评师中级证书、信息安全保障人员认证安全运维(专业级)等认证。现任职于河北翎贺计算机信息技术有限公司技术部，负责网络安全等级测评、风险评估、商用密码应用安全性评估、信息安全审计等工作。刘波先生承担本书部分章节的校对工作。

**何迎杰，**获得河北工业大学通信工程专业工学学士学位，持有国家互联网应急中心 CCSC 讲师认证等认证，中国计算机学会 CCF 会员，现任职于河北翎贺计算机信息技术有限公司技术部，负责网络安全等级测评、风险评估、商用密码应用安全性评估、信息安全审计等工作。何迎杰女士承担本书部分章节的校对工作。

本书原文涉猎广泛，内容涉及云计算安全的各方面的认证考试相关难点，特别是细分领域的安全术语和概念，中文译本极易混淆，往往令应试者考场失利。在本次翻译工作中，针对此类情况，举行了专项学术讨论，(ISC)²上海分会的诸位安全专家给予高效专业的解答，这里衷心感谢(ISC)²上海分会理事会和(ISC)²上海分会会员的参与、支持和帮助。

# 关 于 作 者

**Daniel Carter**，持有 CISSP、CCSP、CISM 和 CISA 等证书，是约翰斯·霍普金斯大学医学院的高级系统工程师。作为一名 IT 安全和系统专家，Daniel 在基于 Web 的应用程序和基础架构，以及 LDAP、PKI、SIEM、Linux/UNIX 系统、SAML 和联合身份系统等领域拥有丰富的工作经验。Daniel 拥有美国马里兰大学的犯罪学和刑事司法学位，以及技术管理硕士学位，研究方向是国土安全管理。

# 关于技术编辑

**Gerry Sneeringer**，持有 CISSP 证书，在过去 32 年一直担任美国马里兰大学的 IT 专家。Gerry 曾参与客户支持、系统编程、系统管理(包括 Internet 根域名服务器之一的运营)和网络工程。在过去 17 年，Gerry 一直是大学中央信息技术办公室的安全主管。Gerry 目前担任该校首席信息安全官职务，负责保护本地和云端的大学计算服务。Gerry 拥有马里兰大学计算机科学学士学位。

# 致　谢

本书是上一个版本的升级版；我十分荣幸地成为这个新版本的作者，开启了自己的写作之旅。首先感谢 Matt Walker 给了我这次机会，并鼓励我抓住这次机会。我希望考生们能从本书中找到有用且全面的信息，从而在他们的职业发展和成长过程中获得帮助。

感谢 Gerry Sneeringer 作为本项目的技术编辑所付出的辛勤劳动，更重要的是感谢 Gerry 在 20 多年来向我传授的知识和经验。我原本没有网络背景，缺乏这方面的专业知识，我在这个领域所拥有的知识几乎完全归功于 Gerry。感激 Gerry，感谢他让我从系统管理和中间件系统的工作转入 IT 安全领域。

我曾在马里兰大学与 David Henry 共事多年，并从他那里学过许多关于中间件和系统架构的知识。我现在已经总结出一套战胜挑战的哲学和思路，这在很大程度上归功于我和 Henry 一起工作时学到的知识和经验。在马里兰大学工作时，我从多位专家那里学到很多知识，此处列出其中几位：John Pfeifer、David Arnold、Kevin Hildebrand、Prasad Dharmasena、Fran LoPresti、Eric Sturdivant、Willie Brown、Sonja Kueppers、Ira Gold 和 Brian Swartzfager。

在医疗保险和补助服务中心工作期间，我要特别感谢 Jon Booth 和 Ketan Patel 给我的机会；他们给了我安全方面的第一个正式岗位，他们充分信任我，安排我监督重要的公共和可视化系统。感谢 Zabeen Chong 给了我加入 CMS 的机会，让我能拓展自己的学术视野。最后，我不能不提及我的好友 Andy Trusz，从我加入 CMS 的第一天起，他就向我展示了工作技能，并成为我非常亲密的朋友。不幸的是，就在我离开 CMS 去 HPE 公司任职的那一天，Trusz 在与癌症的斗争中失败了，他离我而去。我永远不会忘记 Trusz 的深挚友谊和给予我的一切帮助！

对于撰写本书这种规模的项目，往往需要老板和同事们的大力支持和理解。Ruth Pine 是一个很棒的老板，Pine 始终支持我，给我时间和鼓励，使我可以坚持从事这个项目，也一直给我机会让我应对新的挑战和扩展专业领域，特别是云计算技术和 SIEM 技术领域。感谢 Brian Moore、Joe Fuhrman、Steve Larson、BJ Kerlavage、David Kohlway、Seref Konur 和 Jack Schatoff 以及前面提到的 Matt Walker，感谢他们加入 HPE 这样一个令人钦佩的团队，并向我展示了如此多的不同视角和应对挑战的新方法！还要感谢多年来与我在项目上密切合作过的其他公司的伙伴，感谢他们对我的支持和鼓励，特别是 Anna Tant、Jason Ashbaugh 和 Richie Frieman。

两年前，我有机会重返教学岗位，在约翰斯·霍普金斯大学从事一份富有挑战性的工作，我与企业级身份验证团队共同从事 SSO 和联合身份系统工作。与一家大型医院合作，这是一个将我在医疗保健方面的工作经验结合起来的理想机会。

我想借此机会感谢总监 Andy Baldwin，感谢经理人 Anthony Reid 以及与我共事的优秀团队成员：Kevin Buckley、Stephen Molczyk、John Clark、Brian Schisler、Michael Goldberg 和 Sam Bennett。还要感谢 Etan Weintraub、Tyge Goodfellow、Eric Wunder、Steve Metheny 和 Phil Bearmen，感谢他们从许多不同方面向我传授新的安全知识！

感谢父母 Richard 和 Susan，感谢你们的支持和鼓励！最后，也是最重要的一点，我要感谢我伟大的贤内助 Robyn，感谢她一直支持我在职业和个人生活中所做的一切。我们育有四个年幼的孩子，如果没有 Robyn 的理解和帮助，我根本无法完成这个项目，试想一下，如果宝宝们和狗狗们一起在家里四处跑动，我相信，没有专家能完成如此规模的写作项目！

# 前　言

过去几年间，“云(Cloud)”流行开来，即使是那些与 IT 行业没有直接联系、没受过培训或没有专业知识的外行人士，也开始对其熟悉起来。云计算不时出现在面向普通大众的商业广告中，作各类服务的主要卖点。即使是那些不了解什么是云计算(Cloud Computing)或云计算工作原理的人们，很大程度上也认识到云计算是对产品或服务起主要作用的积极因素，普遍认为云计算意味着更高的可靠性(Reliability)、更快的速度和更便捷的整体消费者体验。由于云计算具有诸多优势和特性，如今的许多组织都在鼓足干劲、快马加鞭地拥抱云计算技术。

随着行业运营模式的巨大转变，各类组织对深入、娴熟掌握云计算技术的专家的需求以同样的速度激增，这种需求遍及各个计算领域。由于云计算的独特影响力和特征，使相关组织对云计算安全专家的需求变得分外急迫，以全面保护组织的各类系统(System)、应用程序(Application)和数据。

云计算代表 IT 专家和安全专家看待数据保护以及可用的各类技术和方法的范式转变。在想要获得 CCSP 认证的考生中，一部分是经验丰富的安全专家，并已持有多个安全类证书，如 CISSP 认证等。但对于其他读者而言，这将是成为安全专家的第一次认证考试历程。一些考生早先就开始使用云计算技术，而其他大部分考生则是第一次学习云计算技术的基础知识。本书旨在满足各类考生的需要，不论其是否具有安全或通用计算方面的背景或具体经验。[1]

本书将为考生提供通过 CCSP 考试所需的信息和知识，也将扩展考生对云计算和安全技术的理解和认知，而非仅是应试和答题。希望考生能将本书作为一本案头必备书籍，即使在考试后也继续通过本书更深入地理解核心云计算概念和方法。

本书的结构与(ISC)²官方考试大纲的主题密切相关，涵盖其中的所有目标和组成部分。在深入研究 CCSP 考试涉及的六大知识域前，本书为那些将 CCSP 作为第一项安全认证的考生提供关于 IT 安全的一般性介绍。而那些经验丰富并已持有各类安全证书的考生将发现这是一种复习基本概念和术语的有效方法。

不论考生的背景、经验如何，也无论已持有多少证书，作者都希望考生能通过本书发现云计算领域独特的安全挑战，获得更多启发和顿悟。云计算技术代表计算领域的一个不断发展、令人兴奋的新方向，在可预见的未来，云计算技术将成为一种主要范式(Major Paradigm)。

1　译者注：CCSP 考试借鉴了部分 CISSP 知识体，请考生务必熟读《CISSP 权威指南 (第 8 版)》的知识点。

# 目　录

第1章

# 获得 CCSP 认证的途径及安全概念简介

本章涵盖以下主题：

- 为什么 CCSP 认证的价值如此之高
- 如何获取 CCSP 认证
- CCSP 六大知识域简介
- 基础安全概念简介

随着云计算技术的逐步普及和大规模运用，组织对于安全技能娴熟且具备云计算专业知识的安全专家(Security Professional)的需求量随之增加。虽然组织已聘用大量安全专家和 IT 运营专家，但其中很多专家仅掌握传统数据中心的知识、技能和经验，不能完全应对云计算的独特挑战和特性。为弥补这一差距，$(ISC)^2$ 和云安全联盟(Cloud Security Alliance，CSA)合作推出 CCSP(Certified Cloud Security Professional，认证云安全专家)认证考试，以此鉴定云安全专家的知识和技能，并提供在云环境保证组织安全性所需的培训和教育。

## 1.1 为什么 CCSP 认证的价值如此之高

安全专家一旦获取备受尊崇和认可的行业标准认证，个人职业生涯将获得极大助力。随着云计算技术的高速发展，越来越多的组织呼吁充分利用云计算的潜能，CCSP 认证将作为一个独立机构向雇主或监管机构证明考生已获得足够的云安全技能且正确理解云安全相关概念。CCSP 认证可使各级别 IT 安全从业人员受益，如担任基础岗位的安全分析师或组织的首席信息安全官(Chief Information Security Officer，CISO)。虽然 CCSP 认证在特定情况下作为

其他安全认证的延伸，但这并不妨碍 CCSP 认证作为第一个云安全认证或独立认证的地位；典型的安全认证包括 CISSP(Certification for Information System Security Professional，信息系统安全认证专家)[1]。

## 1.2 如何获取 CCSP 认证

以下是撰写本书时，CCSP 认证考试步骤和要求的最新信息，但由于 IT 行业是一个快速变化的环境，考生应在考前直接与(ISC)$^2$ 确认最新的考试要求。CCSP 认证考试网站为 https://www.isc2.org/ccsp。

获得 CCSP 认证的要求如下。

### 1. 经验

考生至少具有五年的全职 IT 工作经验。在这五年内，考生必须至少有三年的 IT 安全经验，有至少一年在至少一个 CCSP 知识域的工作经验。如果考生拥有 CSA 颁发的 CCSK(Certification of Cloud Security Knowledge，云计算安全知识认证)证书，则 CCSK 证书可替代 CCSP 知识域经验要求，而且(ISC)$^2$ 的 CISSP 认证可单独用于满足 CCSP 认证的全部经验要求。即便考生还没有足够经验，考生仍可参加考试，成为(ISC)$^2$ 准会员。作为(ISC)$^2$ 准会员，将有六年的时间获得所需的知识域经验，并成为一名持证的常规会员。

### 2. 考试

考生需要注册并通过 CCSP 认证考试。有关注册和所需费用的信息可在 CCSP 网站上查询。考试将持续三个小时，共有 125 道题目。总分 1000 分，考生得分 700 分及以上，则被视为成功通过考试。

### 3. 遵守(ISC)$^2$ 道德规范

作为安全专家团队的成员，任何 CCSP 持证人士都必须同意并遵守最高的职业和道德标准。有关道德规范，请参见 https://www.isc2.org/Ethics。

### 4. 背书

在达到经验要求并成功通过考试后，考生的申请必须得到当前(ISC)$^2$ 认证持证人士的背书(Endorsement)。背书需要由认识考生并能证明考生专业经验和资格有效性的持证人士完成签字程序。

### 5. 证书维护

获得 CCSP 认证证书后，持证专家必须完成特定的继续专业教育(Continuing Professional

1 译者注：建议 CCSP 考生仔细阅读《CISSP 权威指南(第 8 版)》提及的每个知识点。

Education，CPE)，并支付年度维护费(Annual Maintenance Fee，AMF)。有关这两项要求的最新信息，请参阅$(ISC)^2$官方网站 www.isc2.org。

# 1.3　CCSP 六大知识域简介

CCSP 考试内容分为六个不同但又相互关联的知识域(Domain)，涵盖宽泛的但与云计算紧密相关的安全和运营问题。六大知识域的考试权重如图 1-1 所示。

**CCSP考试权重**

| 知识域 | 权重 |
| --- | --- |
| 1. 云概念、架构与设计 | 17% |
| 2. 云数据安全 | 19% |
| 3. 云平台与基础架构安全 | 17% |
| 4. 云应用程序安全 | 17% |
| 5. 云安全运营 | 17% |
| 6. 法律、风险与合规 | 13% |
| 合计: | 100% |

图 1-1　CCSP 六大知识域考试权重

## 1.3.1　知识域 1：云概念、架构与设计

“云概念、架构与设计”知识域为深入掌握云计算的必备知识奠定基础。这些构建块(Building Block)基于 ISO/IEC17788 标准。该知识域从云服务提供商和云服务客户的角度定义个人和其他实体在云实现过程中扮演的不同但关键的角色。该知识域概述云计算的关键特性，包括按需自服务(On-Demand Self-Service)、多种网络访问方式(Broad Network Access)、多租户(Multitenancy)、快速弹性(Rapid Elasticity)、可伸缩性(Scalability)、资源池化(Resource Pooling)和可计量服务(Measured Service)。该知识域还介绍云环境的关键构建块，如虚拟化技术(Virtualization)、存储(Storage)、网络(Network)以及承载和控制上述部分的底层基础架构(Infrastructure)。

“云概念、架构与设计”知识域涵盖云参考架构，介绍云计算活动、云服务能力、云服务类别(Category)、云部署模型以及影响云实现和部署的所有知识域的云计算的交叉方面。云计算活动基于 ISO/IEC17789 标准，包括云服务提供商(Cloud Service Provider，CSP)、云服务客户和云服务合作伙伴的关键角色，以及每个角色下封装的各种子角色。介绍并定义了主要的云服务功能，包括应用程序、基础架构和平台服务功能，因为上述内容构成了许多常用和可理解的云架构和模型的基础。在云服务功能后，介绍主要的云服务类别，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)。云服务类别也可存在于不同的云部署模型中，包括公有云、私有云、混合云和社区云。云参考架构(Cloud Reference Architecture)的最后一个组件是适用于所

有云环境的云计算交叉方面(Cross-cutting Aspect，指贯穿云计算研发和使用过程的通用安全要素)的集合，而无论何种云服务类别或云部署模型，始终贯穿其中。这些交叉方面包括互操作性(Interoperability)、可移植性(Portability)、可逆性(Reversibility)、可用性、安全性、隐私性、韧性(Resiliency)、性能、治理、维护和版本控制、服务水平、服务水平协议(Service Level Agreement，SLA)、可审计性(Auditability)、法律法规和监管合规。该知识域还探讨新技术对云计算的影响，如机器学习、人工智能、区块链、容器和量子计算。

对于任何托管环境(Hosting Environment)而言，安全概念都是重要且核心的要素，但云计算环境还有一些值得特殊考虑的因素。不仅如此，有很多安全概念也是云计算技术所独有的。与任何数据中心环境一样，安全对于网络安全、访问控制、数据和介质脱敏、加密和虚拟化技术都至关重要。所有这些应用场景都与传统数据中心模型非常相似，但在具有多租户(Multitenancy)的云环境中，加密的重要性显著提升，因为云环境与传统的数据中心的独立部署模式相反，多个云客户都处于相同的资源池中。这同样适用于云端处理数据和介质脱敏(Sanitation)的独特安全挑战，即在云环境中访问和处理物理介质不可行也不实用。随着云计算采用虚拟化和物理硬件的抽象化技术，与传统的数据中心模型相比，对虚拟机管理程序(Hypervisor)安全和容器安全的重要性提出新的挑战。本书介绍了云计算面临的常见安全威胁，这是由 OWASP(Open Web Application Security Project，开放 Web 应用程序安全项目)发布的，同时讨论了不同的云计算类别(IaaS、PaaS 和 SaaS)面对的整体安全挑战以及每类云计算所面临的独特安全挑战。

云计算安全有特定的设计要求。虽然与传统数据中心存在部分重叠，但云环境的特性决定了很多设计方面需要采用特殊的考虑因素或方法。例如，适用于云安全数据生命周期，以及云环境中业务持续性和灾难恢复(Business Continuity and Disaster Recovery，BCDR)的不同方法。有了这些不同的方法和考虑因素，组织需要执行成本效益分析(Cost–Benefit Analysis)活动，包括运营变化、策略变化、监管挑战，以及迁移到云环境所需的任何配置变化，甚至需要考虑组织是否应迁移到云端。该知识域还介绍云计算的安全功能需求，包括互操作性、可移植性和供应商锁定(Vendor Lock-in)。

最后，知识域 1 还深入研究第三方认证作为向云计算体系传递信任的一种方式。因为云客户并未托管和控制整个云环境，云客户只能寻求其他方法来验证云服务提供商的安全态势和运营风险水平，而一种简单且可信赖的方法就是审查独立测试和验证的第三方认证。第三方认证服务商的工作是基于已发布且受到广泛支撑的标准和要求；第三方认证报告是云客户信任云服务提供商安全态势和控制措施的一种手段，同时为对比不同的云服务提供商提供一种通用方法。第三方认证可针对整个环境和应用程序开展活动，也可集中在特定的组件和服务上。通用准则(Common Criteria，CC)是一种已广泛采用的国际安全标准，而其他第三方认证和标准(如 FIPS 140-2)则侧重于特定的加密模块及其安全性和验证。

### 1.3.2　知识域 2：云数据安全

“云数据安全”知识域深入研究系统和应用程序的设计、原则和最佳实践如何保护数据，同时考虑托管环境中所有类型的系统、服务、虚拟机(Virtual Machine，VM)、网络和存储技术等。知识域 2 首先讨论云数据生命周期(Cloud Data Lifecycle)，展示数据的创建乃至废弃过程，以及如何在系统或应用程序中通过各种用途和活动处置(Handle)数据。

每个云类别(IaaS、PaaS 和 SaaS)都有与之相关并由其使用的不同类型和存储方法。该知识域解释了 IaaS 的卷和对象存储类型、PaaS 的结构化和非结构化数据类型、信息和存储管理，以及 SaaS 的内容和文件存储可能性。每种类型的存储都会带来特定的安全挑战，但解决这些问题的策略通常是相似和统一的，包括加密技术(Encryption)和数据防泄露(Data Loss Prevention，DLP)等策略。

在云环境中用于确保数据安全的技术与传统数据中心的技术类似；只是由于云环境中的多租户和虚拟化技术而变得越来越重要。主要使用的数据安全方法是加密技术，包括密钥管理、哈希运算、掩蔽(Masking)、混淆(Obfuscation)、标记化(Tokenization)和数据反识别(De-identification)的重要方面。具体技术的确切使用方式，包括如何使用以及范围是什么，将取决于正在处理或存储的数据类型、数据分级分类(Classification)、针对特定安全控制措施或安全策略的法律法规和监管合规要求。知识域 2 还涉及若干新安全技术，如同态加密(Homomorphic Encryption)，分析这些新技术在未来通用数据安全(特别是云端数据安全)中扮演的潜在和重要角色。

对于任何类型的数据安全，数据探查(Data Discovery)和数据分类的流程都很重要。数据探查包括查找系统或应用程序中存在的数据并使其发挥价值，以及确保所有数据都是已知的，并部署适当的安全控制措施。在云环境中，数据探查更加复杂且更为重要，因为数据存储在完全不同和多种多样的系统上；数据所有者(Data Owner)和云客户(Cloud Customer)甚至可能无法完全知晓数据的确切地理位置。一旦数据已知，数据分类就可根据数据的属性确定所需的适当安全控制措施和策略的流程。数据分类规则可来自组织策略、法律法规和监管合规要求。在云环境中这一点越来越重要，因为多租户环境可能导致云租户将数据暴露给未授权实体。

许多数据的分类(注意，业内人士采用更啰嗦但更规范的说法，即“分类分级”。本书后面提到“分类”时，即指“分类分级”)，特别是处理个人身份信息(Personally Identifiable Information，PII)的分类，往往都由特定的司法管辖权要求或控制措施所驱动。这源于各式隐私法案，这些隐私法案规定了必要的数据探查和数据分类的流程。设计精妙的控制措施可映射并满足特定司法要求；但个人身份信息的特殊子集，如个人健康信息(Personal Health Information，PHI)等，可能需要额外的控制措施和特殊处置。

保护数据的两种主要方法是数据版权管理(Data Rights Management，DRM)和信息版权管理(Information Rights Management，IRM)。DRM 适于保护用户介质，而 IRM 则适于保护系统端的信息。DRM 和 IRM 概念和实现概念的特定工具可用于制定以下策略：持续审计、访

问有效期、策略控制、保护以及支持许多不同的应用程序和数据格式。DRM 和 IRM 都允许比典型的系统或应用程序数据控件更细的粒度和更高的控制水平。

对数据策略而言，留存(Retention)、删除和归档(Archive)等概念都非常重要。许多法律法规和监管合规要求都明确组织需要制定数据(尤其是日志)的数据留存策略(Data Retention Policy)，并由组织和数据所有者决定合规性所需的策略和技术。对于归档系统，都必须确保在任何留存策略或法规的有效期内正确创建并保护归档，且可访问和读取这些归档。必须以全面、安全的方式清洗(Clear)要从系统中移除的数据，以确保以后未授权各方无法恢复和访问这些数据。该知识域还介绍数据留存的一个特殊类别，即以特定格式或状态保存数据供合法持有。

最后，数据安全的关键组件之一是记录来自系统和应用程序的特定且详细的事件(Event)，包括系统级别和应用程序级别的事件和日志，并且应该根据特定类型的数据或应用程序来确定事件类型和细节。法律法规和监管合规要求是确定事件类型和所需细节的要素。此类事件集合可用于监管合规性、监督(Oversight)安全性、利用业务智能和系统资源。大多数组织都集中收集日志，并使用聚合(Aggregation)技术执行分析。与任何类型的数字证据和数据一样，对于事件日志以及存储和保存事件日志的系统而言，采用特定安全机制保护证据保管链(Chain of Custody)和抗抵赖性(Non-repudiation)至关重要。

### 1.3.3 知识域 3：云平台与基础架构安全

云环境由物理基础架构(Physical Infrastructure)和虚拟基础架构组成，两者都带有特定的安全问题和需求。虽然云系统建立在虚拟化和虚拟组件之上，在虚拟化层之下是物理硬件及其对应的安全需求，与传统的数据中心没有差别，包括对物理系统(如 BIOS 和硬件层)的访问，以及承载和维护其上的虚拟化环境的软件。任何违反物理层安全性或控制的行为都可能使在其中管理的所有虚拟主机也处于风险之中。云环境中的安全控制措施适用于各种标准资源集：网络和通信、存储和计算。然而，使用虚拟化技术时还需要考虑用于控制虚拟机的管理平面安全性。知识域 3 深入研究云计算特定风险、虚拟化相关风险，以及可部署的特定安全对策战略。

随着云计算广泛用于连接各个组织并为大量用户提供服务，身份和访问管理(Identity and Access Management，IAM)是 CCSP 持证专家必须精通的重要安全概念之一。IAM 涵盖的主题包括准确辨识合法用户、常用于验证用户身份并证明其身份符合安全策略或法规要求的安全机制。一旦证实用户身份的合法性，就需要执行严格的授权控制措施，以确保用户只访问已授权的信息，且通过授权的方式访问这些信息。在许多基于云技术的系统中，一种常用方法是联合身份(Federation Identity)，用户可通过自己组织的身份服务提供商执行身份验证流程，然后让某特定服务提供商接受身份验证令牌(Authentication Token)进而访问系统或数据，而不需要用户在特定系统上创建账户。

知识域 3 最后介绍 BCDR(Business Continuity and Disaster Recovery，业务持续性和灾难恢

复)概念。尽管云平台及其固有冗余措施可缓解多项可能影响传统数据中心的典型停机诱因，但合理的规划和仔细分析仍然至关重要。对于完全部署在云环境中的应用程序，互操作性(Interoperability)和可移植性(Portability)使组织能利用其他云服务提供商或同一云服务提供商中的其他产品来实现 BCDR 战略。即使仍然驻留在传统数据中心的应用程序也可使用 BCDR 的云产品，特别是考虑到云服务只在使用时产生成本，从而减少了对备用硬件的需求。为实施适当的 BCDR 战略，规划阶段至关重要，但也必须进行定期测试，以确保所有组件仍然适用且可行。

### 1.3.4　知识域 4：云应用程序安全

云环境和云技术因其成本和灵活性而迅速流行起来。云环境为开发人员提供了难以置信的效率和便捷，可快速地为开发人员带来在线环境和虚拟机，而且只有在线环境和虚拟机处于运行状态时才会产生成本。在云环境中，与传统数据中心中采购环境或测试服务器相关的交付时间和成本压力在很大程度上得到缓解。为使用最优的云研发环境，特别是考虑到安全性，云安全专家和研发团队需要充分掌握云环境的真实情况、保护环境所需的控制措施以及云环境面临的常见威胁和漏洞。

虽然不是云托管或研发部门所独有的，但知识域 4 讨论不同类型的应用程序测试和扫描。测试和扫描类型由不同的方法和视图组成，且结合使用，允许对系统和应用程序执行详尽且全面的测试。通常认为，动态应用程序安全性测试(Dynamic Application Security Testing，DAST)是“黑盒(Black-box)”测试，用于测试已投产系统而不必了解系统的全部知识和配置。而静态应用程序安全性测试(Static Application Security Testing，SAST)是在完全掌握系统配置以及有权访问源代码情况下进行的，并且是针对非投产系统(Non-Live System)开展的测试活动。渗透测试(Penetration Testing)使用与攻击者同样的方法和工具集，用于确定系统漏洞(脆弱性)，而运行时应用程序自我保护(Runtime Application Self-Protection，RASP)则侧重于系统和应用程序在发生攻击时自我保护和阻止或减轻攻击的能力。

由于大多数现代应用程序，特别是那些通常在云端部署的应用程序，都建立在使用其他服务和数据的组件、服务和 API 的基础上，因此选择和验证满足安全需求的适当部分是至关重要的。关于“最弱环节”的古老话题在这种情况下依然是有效的，因为单个组件的任何弱点都可能使整个应用程序或系统面临威胁和利用。无论组件的来源是什么，都可使用相同的验证流程和选项，包括商业、开源和社区源代码的应用程序。

知识域 4“云应用程序安全”涵盖与云环境相关的软件开发生命周期(Software Development Lifecycle，SDLC)，包括每个阶段的深入演练、所需的内容、在进入下一阶段前需要处理的关键组件，以及 SDLC 的周期性。介绍 STRIDE 和 DREAD 模型中的主要威胁和脆弱性(亦称漏洞)概念，包括 STRIDE 模型和 DREAD 模型在云环境中的适用性。

在安全软件研发概念和方法的基础上，还介绍了云计算中其他常用的技术和范例。其中包括 XML 专用工具包、Web 应用程序防火墙(Web Application Firewall，WAF)和系统化方法，

如沙箱和应用程序虚拟化技术。文中还讨论了这些常用的技术和范例在云计算中的重要性以及对密码技术的基本用途和依赖性。最后，知识域 4 涵盖了身份和访问管理的战略方法，并在实现过程中将其构建为应用程序，包括多因素身份验证(Multifactor Authentication，MFA)技术。

### 1.3.5 知识域 5：云安全运营

“云安全运营”知识域首先讨论数据中心的规划问题，包括物理层和逻辑层及所采用的各种技术，还包括如何处理环境风险和需求以及物理需求，如可靠且冗余的冷却和电力资源，及充分予以保护以免受自然灾害和环境风险的影响。

尽管在大部分人眼中，云环境就是以虚拟化方式运营的，但云环境依然继承了传统数据中心的底层物理环境和相应的风险，即便这些安全风险已经由云服务提供商处理和维护，但在很大程度上这些担忧是从云用户和云客户的观点和关注中抽象出来的。物理层由托管虚拟化环境的服务器以及存储和网络组件组成。从网络的角度看，传统数据中心的全部问题依然存在，如防火墙、路由器和基于网络的入侵检测和防御系统。物理设备也可在独立配置或集群配置中运行，这取决于环境的特定关注点或特定的安全需求和期望。物理环境在云环境中也具有许多与传统数据中心中的服务器相同的要求，包括补丁管理和版本控制、访问控制、日志收集和保存以及审计要求。由于物理环境对虚拟化环境有直接影响，因此需要对维护和管理活动进行全面规划和调度。

在很大程度上，逻辑环境与物理环境承担着相同的风险和要求，但不同的是，逻辑环境的关注点在云客户的系统和应用程序上，如在云环境中使用的实际虚拟机和网络设备。云环境的各类系统还需要补丁管理和版本控制策略，但根据所用的云模型，这种方法可能与传统数据中心模型有很大不同。逻辑环境需要强大的性能持续监测能力，由于负载和需求不断变化，需要考虑物理环境的性能、系统如何动态平衡以及如何在物理系统之间分配资源，以保持最佳性能。逻辑环境还需要考虑逻辑系统的备份和恢复。

知识域 5 全面涵盖 ITIL 的组件和概念，ITIL 是一组 IT 服务管理的最佳实践，在整个 IT 行业中广泛使用，因为 ITIL 形成一种可运用于任何系统或应用程序的全面的运营管理方法。本书讨论了其中十个主要组件，包括 IT 系统和服务工作人员都非常熟悉的组件，如变更管理(Change Management)、配置管理(Configuration Management)和信息安全(Information Security)管理。

云安全运营的另一个重要部分是收集和保存电子记录，以用作数字证据。这些系统和程序代码需要成为运营方案不可缺少的组成部分，而不是只有在需要时才加以解决的工作。知识域 5 从入门级运营角度介绍这些主题，并将讨论扩展到知识域 6 中包括的监管角度。

知识域 5 涵盖与利益相关方(Stakeholder)的适度沟通，这是运营活动的一个重要方面。利益相关方包括参与人员或合同范围内的所有级别的人员，如供应商、客户、合作伙伴、监管机构，以及基于数据、应用程序或系统细节的其他任何潜在利益相关方。恰当且有效的沟通

对于培养和维持牢固的关系十分重要，根据合同、服务水平协议(Service Level Agreement，SLA)或法规的要求，可能需要在服务频次和细节水平方面进行具体沟通。

最后，知识域 5 涉及组织内部安全运营的管理工作。这包括建立一个安全运营中心来监测组织的技术和运营安全需求。随着安全控制措施的部署，必须实施各种机制来持续监测这些控制措施，确保这些措施不会在正式程序和批准之外发生变化，并确保这些安全控制措施按照设计和预期的方式工作。以集中的方式收集和维护日志数据，以便对事件进行关联和持续监测。为覆盖所有安全事件(Event)并对任何事故(Incident)做出响应，应建立强有力和用于安全管理的事件和事故管理流程和团队。

### 1.3.6　知识域 6：法律、风险与合规

“法律、风险与合规”知识域关注 IT 系统的法律法规和监管合规要求，包括 IT 系统的法律法规和监管合规要求如何与云计算及其许多独特方面的深度联系。云计算技术带来许多特有的风险和挑战，因为云计算环境常跨越不同的监管体系或国家边界。因此，云计算受到许多不同的法律法规和监管合规要求的制约，有时，这些不同体系的法律法规和监管合规要求还会相互冲突。知识域 6 从多个不同司法管辖权区域的角度探索法律法规强制控制，以及云计算特有的法律风险。涵盖与司法管辖权(Jurisdiction)控制相关的个人信息(Personal Information)和个人隐私的具体定义和法律要求，以及根据合同规定的个人数据保护和受监管的个人数据保护之间的区别。

对任何 IT 系统或应用程序最常见的法律影响是电子取证的指令和要求，即根据正式的法院命令或请求生成记录或数据。知识域 6 探讨了电子取证(eDiscovery)和数字取证(Digital Forensics)的总体概念，特别是当这两种取证类型与云计算和云平台所代表的特定挑战相关时。安全专家熟悉的这两个知识域的许多工具和流程在云环境中并不直接可行，由于云客户将不具备执行数据收集所需的访问类型，因此必须通过合同和其他正式流程来处理这些请求。

IT 安全性和法规合规性最重要的方面之一是审计流程(Auditing Process)。知识域 6 从监管角度研究了各种类型的审计、审计的目的和需求，及其对云计算的具体影响。云计算技术的主要挑战之一就是代表云客户查看和访问底层基础架构，以及云服务提供商如何使用审计和审计报告来确保多个客户对安全计划的信心，而不需要给每个客户访问权限或执行多次类似的基础架构审计。知识域 6 广泛涵盖了围绕审计和认证(Certification)的标准、常用的审计模型和报告、每种模型和报告的适当用途和受众，以及准确识别相关利益相关方。

知识域 6 中还深入探讨了风险管理(Risk Management)，以及风险管理在云计算方面的具体运用和关注点。引入云计算技术后，失去直接控制权将成为组织内部风险管理的主要问题，需要特殊的评价(Evaluation)和理解机制。包括各种风险管理流程和程序，以及不同的风险框架和评估方法。这个风险评估流程包括四个阶段：建立、评估、响应和持续监测。按顺序建立每个阶段，从定义过程和风险类别开始执行评估，确定适当的应对措施或接受已识别的任何风险，然后持续监测这些风险，以备将来的发展或应对战略的变化。总体而言，可以接受、

避免、转移或缓解风险，或者可以组合使用这些方法。

知识域 6 最后涵盖管理和确定云托管合同范围的各项关注点和具体需求。这包括选择云服务提供商的指导，以及需要在合同中解决的关键组件和问题，这些是特定于云托管的问题以及云客户将要关注的问题。

# 1.4 IT 安全简介

尽管许多申请 CCSP 认证考试的考生已经持有其他主流的安全认证证书，如 CISSP 等，但这不是 CCSP 报考的硬性要求。下面简要介绍对所有安全专家而言都不可或缺的基本安全概念，其中包括风险管理、业务持续性和灾难恢复(BCDR)概念等。如果考生在 IT 安全方面具有丰富经验或持有其他主流认证证书，请略过这一节，可直接学习第 2 章，即 CCSP 考试涉及的第一个知识域。然而，即便考生是一名经验丰富的安全专家，也会发现下述知识点极具价值；如果考生正在备考职业生涯中的第一个安全认证，将发现这些尤其有用。

## 1.4.1 基础安全概念

在不考虑用途或技术细节的情况下，以下基础安全概念适用于所有系统和应用程序。

### 1. 最小特权

IT 安全领域的主要驱动原则是“最小特权(Least Privilege)”。最小特权原则的基础是：仅允许用户以符合目的和明确授权的方式对系统、应用程序或数据进行访问。例如，对系统具有管理级别权限的用户只应在绝对必要时才使用管理级别的访问等级，并且只在所需的特定功能和时间周期内使用管理级别权限。用户(User)应该使用正常的用户访问权限执行日常操作，并且只有在必要时才提升到管理级别的访问权限。在执行完必要功能后，管理级别权限应立即返回到用户状态。

组织遵守最小特权最佳实践可获取多项安全和运营方面的收益和成果。首先，最小特权最佳实践可防止用户长时间使用管理权限执行访问操作，这种情况下，失误或错误命令的可能性对系统产生诸多负面影响。最小特权最佳实践还可防止在没有其他独立验证或要求的情况下，使用管理权限执行访问操作，避免因账号泄露而对系统产生的负面影响。许多情况下，管理访问权限将限制在某些访问手段上，例如，要求用户仅在其组织网络上使用管理访问权限，这是因为在组织网络上有其他防御安全措施可用于缓解风险。使用多因素身份验证(或单独且不同的安全凭证)来加固管理权限账号也是常见做法。由于需要额外的安全凭证，即使用户泄露口令，攻击者想要实现管理级别的访问也需要进一步的攻击行为，因此成功检测或预防攻击活动的概率将更高。

同样的概念也适用于环境或应用程序中使用的服务或系统账户，例如，Web 服务器、应用程序服务器和数据库等组件都作为特定系统账户在系统上运行。与用户账户非常类似，这

些系统账户也应该在只向其分配所需最低级别权限的情况下生效。这有助于分离和隔离系统上的应用程序进程，并防止进程在没有明确授权的情况下访问其他数据或进程。例如，应创建和利用特定于这些应用程序或进程的单独账户，而避免使用系统的 root 或 admin 账户执行进程。当进程在具有过大访问权限和特权的账户下运行时，一旦攻击者攻克并控制进程，恶意攻击者将自动获得对系统、系统包含或运行的任何数据，以及其他进程的越权访问权限。

虽然大多数特权与读取数据的能力相关联，但特权也包括更新系统文件的能力。除非明确需要，否则服务和进程不能在文件系统上写入或修改文件。如有必要使用此项功能，则必须采取步骤限制写入和更新的位置，并且这类操作应尽可能隔离和限制。任何服务都不能更新(Update)系统上的二进制文件或应用程序配置，以防止引入和执行特洛伊木马或恶意软件。一个明显且常见的例外情况是允许进程将日志文件写入系统，但这也应限于特定的位置或文件，并应通过文件系统权限或特定于环境的其他安全设置来强制执行访问。

在任何环境中，最小特权的真实系统或环境都很棘手。组织不可能完全构建特定进程只用于其所需的确切访问水平的细粒度，这是因为，系统是建立在公共库和配置的基础之上，运行在系统上的所有进程都需要访问或执行这些库和配置文件。关键在于确保敏感数据和功能不会发生非授权公开，以及确保流程在没有明确需求和缺少正式授权的情况下无法更新或删除数据或配置。所有访问都需要在组织的风险管理流程中进行评价(Evaluate)，并在授权之前记录和批准特定的访问权限。

### 2. 深度防御

深度防御(Defense in Depth)的前提是使用多层次和不同类型的技术和战略为组织提供安全性。有了多层防护机制，任何一点上的故障或漏洞都可通过部署的其他安全机制和系统得到缓解或将后果最小化。虽然多层安全不能完全消除任何潜在的攻击或成功利用漏洞的可能性，但多层安全将显著增加敌对者攻击成功的难度，或者在攻击活动成功之前更容易发现和预防攻击行为。

可组合使用许多常见的安全防御战略，构成系统或应用程序的深度防御体系。显而易见的出发点是实际系统或应用程序本身的安全性，但在这个关键控制点之前，可以综合使用其他技术，如防火墙、虚拟专用网络(VPN)、入侵检测或防御系统(IDS/IPS)、漏洞扫描、物理安全、日志记录、持续监测以及其他许多方法和防御战略。基于真实系统或应用程序的扫描和审计报告，可选择特定的其他防御战略和安全技术，同时着眼于特定的缓解措施和弱点，以及数据中心已采用的标准深度防御方法。

使用多台单独设备和多项独立技术实现安全性，还可消除特定防御措施之间的相互依赖性，并使成功利用或绕过防御措施变得更困难。例如，如果某应用程序在服务器上使用多种安全软件来进行防护，如防火墙和病毒扫描等，但服务器本身存在管理漏洞，则应用程序进程可能遭到非授权禁用、非法暂停或篡改配置，使应用程序和安全软件变得无法使用。很多时候，由于攻击者可能已完全控制服务器，因此检测此类非授权篡改极其困难。通过使用不在同一服务器上运行的设备和组件以及基于硬件的实现，可有效地消除并发危害的可能性。

虽然这在很大程度上缓解了来自外部的成功利用，但拥有由不同团队和策略管理的独立设备或安全专用工具包也可降低内部威胁的可能性。

### 3. 机密性、完整性和可用性

机密性、完整性和可用性的概念可认为是 IT 安全的基础，也是此后一切安全工作的基础。虽然这三个概念往往一起使用，但根据具体业务需求和监管要求，不同类型的数据在这三个知识域中的重要性会有所不同。

- **机密性(Confidentiality)** 防止非授权方访问或查看敏感数据。安全保护的水平和程度取决于所披露数据的危害或后果，无论是对组织声誉的影响，还是对非授权方披露数据可能产生法律法规和监管合规的后果。促进或加强机密性保护的安全控制措施在本质上是技术性的，但通常也涉及相关策略、最佳实践和安全处置的用户培训。
- **完整性(Integrity)** 在系统或应用程序中始终保持数据的一致性(Consistency)和有效性。完整性确保数据免受任何未授权篡改，如避免数据在传输过程中的非法篡改。虽然访问控制是防止未授权篡改的主要策略，但其他技术(如校验和技术，Checksum)通常用于验证文件或数据是否仍处于其预期形式，并可立即检测出是否对数据进行过更改。
- **可用性(Availability)** 虽然可用性看起来更像是一个运营问题而非安全问题，但安全性的许多方面在可用性中起着至关重要的作用。虽然确保数据处于有效保护状态对于机密性和完整性至关重要，但如果依赖这些系统的授权用户无法使用系统，则对组织没有任何用处。防火墙、入侵保护系统和防止拒绝服务攻击等安全实践都是安全计划(Security Program)的关键组成部分。这还延伸到通过备份和恢复、业务持续性和灾难恢复来防止数据丢失和业务失败的场景。

### 4. 密码术

密码术(Cryptography)是一套使未授权实体无法读取信息的流程，同时允许已授权访问信息的实体能够轻松地阅读信息。密码术本质上是通过使用数学公式和复杂算法来加密明文数据并使其看起来完全是无意义的随机乱码。数据加密和解密流程的基础是合理使用密钥(Key)。持有密钥的实体可轻易地解密数据，而没有密钥则几乎不可能完成解密密文。大多数情况下，只要有充分的时间和足够的计算资源，那么所有加密密文都可破解。加密的强度取决于使用资源、技术和知识来破解加密所需的时间。例如，尽管现代加密系统是可能遭到破解的，但即便使用所需的计算资源，破解也需要数百年甚至数千年的时间。当然，技术、计算能力和数学上的突破时有发生，因此，今天认为安全的加密体系明天可能变得十分脆弱。密码术和密钥的运用场景分为两类：对称(Symmetric)和非对称(Asymmetric)。

对称密钥的实现方式使用同一密钥执行数据加密和解密流程，因此通信双方在开始交换数据前就必须获取可用密钥，但密钥同步流程往往较困难。使用对称加密算法的共享密钥(Shared Key)处理数据加密要比非对称算法的速度快得多。对称加密的使用场景通常限于两个

可信方之间正在进行和已建立的通信，例如，定期或持续使用的服务器到服务器通信和隧道实现场景。

对于非对称(或公钥，Public-key)加密技术而言，使用不同的密钥分别用于通信的加密和解密阶段。虽然非对称算法低于对称算法的加密速度和效率，但非对称加密是最常用的方法，因为在使用时往往并不清楚有多少参与方，如 Internet 用户访问网站时使用的安全通信。公钥加密通信的每一方使用一对密钥，通常称为公钥和私钥。顾名思义，公钥公开可用，由用户交换或发布。与公钥对应的是私钥(Private Key)，私钥相关信息始终由用户安全地持有且从不向外部分发。当需要安全通信时，发送方可使用接收方公钥对数据或通信进行加密。由于公钥是可公开的，因此初始通信不需要是安全信道，而对称加密则与之相反，这也是非对称加密的另一个主要优点。实践中，非对称加密通常用于 Web 和移动应用程序。然后，接收方用自己的私钥(只有接收方自己知道)解密数据或通信信道。也可用相同方法对数据进行数字签名，以验证通信的发送者或发起者，并确保数据在传输过程中免受篡改的威胁。公钥加密体系是 TLS 和 SSL 等常见安全协议的基础。

### 5. 证书

证书(Certificate)是向特定用户证明身份和验证公钥所有权的基础。证书包含有关用户、组织及位置等的信息，而且仅对请求方可见。为确保有效性和信任，证书通常由证书颁发机构(Certificate Authority，CA)进行数字签名和颁发。大多数情况下，这将是一个受用户和应用程序信任的商业供应商。例如，Web 浏览器包含许多认为是可信的 CA 的“根”证书。这些组织建立严格流程，以确保颁发可信证书所需的身份和标准。有了这种第三方信任关系，即使双方先前没有关系，也没有建立凭证交换，也可进行安全和受信任的通信。由于双方都信任 CA，因此可保证彼此的有效性。

虽然共同 CA 的使用非常普遍，但在特定的应用程序和业务场景中，较小社区可能为自己的目的和用户建立自有 CA。例如，一所大学可建立自有 CA，向所有学生颁发证书，保证只有其用户群体才能访问系统，其目的是为了减轻学校购买商业证书的相关成本。在类似场景中，用户可选择信任 CA 的根证书，而不必单独接受个人或系统的每个证书。因此，学校自行发行证书的工作原理与那些根证书以及在CA的授权下签名的所有证书(通常在浏览器中加载)相同。

如果用户试图与不存在可信证书的实体通信，则该用户将在其浏览器或客户端中收到一条警告，说明用户收到的是不可信的证书，或根颁发机构不是可信颁发者。虽然用户可选择覆盖和接受证书，但只有当用户非常明确地知道为什么出现此警告，并且自己知道可信任源时，才应该这样做。对于更大的公共社区或商业网站使用的系统，绝不能这样做。

### 6. 物理安全

虽然有关 IT 系统的大多数安全讨论都是基于硬件和软件解决方案以保护数据安全，但物理资产保护和物理访问控制对 IT 安全也至关重要。物理安全(Physical Security)与 IT 资源和数

据所在的建筑物和物理位置(Location)，以及数据所在物理设备的防御措施相关。IT 安全常用的深度防御(Defense-in-depth)原则同样适用于物理安全。有了物理结构，分层安全体系，如围栏、监视(Surveillance)、安保团队、锁闭的门、加固建筑结构等都起着核心作用。

物理安全故障或物理安全措施不足都将导致组织面对数据丢失或服务失败等诸多问题。最明显的是由于破坏物理资产(如服务器、存储系统或网络连接)而导致的服务停顿。破坏组织物理安全也可能导致攻击者使用物理访问入侵正在运行的系统。然而，即使系统对外围攻击和访问具有强大的安全性，许多情况下，系统仍然容易受到拥有控制台、硬件以及系统本身的物理访问权的人的影响。最后，缺乏实物安全措施可能导致实物资产盗窃事件。虽可采用安全对策来防止恶意人员通过网络访问系统，但如果攻击者设法窃取存储敏感数据的硬件或存储系统，则恶意人员将能通过使用大量工具和方法设法访问数据，且不受时间的限制，也不受其他能阻止恶意访问的机制的限制。

### 1.4.2 风险管理

风险管理过程通过分析和测试确定与组织现有数据和系统相关的特定弱点(Weakness)、脆弱性(Vulnerability，亦称漏洞)和风险。风险管理(Risk Management)还包括确定适当的缓解措施或接受特定风险。风险有许多不同的形式，包括物理威胁、自然或环境威胁、软件弱点和漏洞利用，以及恶意内部威胁。所有组织必须不断评价(Evaluate)所有系统、应用程序和数据的风险，同时要考虑管理层的风险偏好(Risk Appetite)以及管理层愿意接受的风险水平。显而易见，组织不可能完全消除(Eliminate)所有风险，但一个合理的方法是尽可能减轻风险，并将风险发生的可能性和风险可能造成的任何潜在损害降至最低。风险管理决策还受到来自法律法规、监管合规或司法体系的具体要求的指导，以及对非法数据访问或数据泄露的潜在和特定惩罚。

### 1.4.3 业务持续性和灾难恢复(BCDR)

业务持续性和灾难恢复(Business Continuity and Disaster Recovery，BCDR)是为组织处理突然、意外或灾难性的系统或数据丢失事件而制定的方案。BCDR 包括 IT 运营的若干不同方面，包括 IT 系统的韧性恢复能力、从任何损失中恢复的能力，以及处置恢复时间较长的重大事故或灾难。

BCDR 的第一个主要概念是韧性(Resiliency，指快速且自动恢复的能力)。系统和流程(Process)的实施应具有足够的冗余和容量，以便从一开始就能减少多类威胁或隐患，而不会明显影响系统用户的正常操作。BCDR 可通过在各个层面部署冗余的系统和资源来实现，从电源和冷却系统到系统可用性和人员。

BCDR 的第二个主要概念是从中断或系统损坏中恢复的能力。这种情况下，恢复(Recovery)是指物理资源可能仍然可用，并且损失来自系统或环境部分的损坏或物理故障。可

使用备份技术将系统恢复到最近的时间点。恢复的数据量和时间点将由管理层定义，即发生故障或中断时管理层愿意承担多大程度的数据丢失；大多数情况下，服务可在相同的环境中快速恢复。

最后一个主要概念是灾难恢复(Disaster Recovery)，即自然灾害、恐怖袭击、火灾或其他此类重大事故造成的灾难性损失。这种情况下，在可接受时间内从大量损失中恢复是不可行的，因此，往往需要为转移到另一个托管数据中心制定方案并做好准备，在迁移规划中，数据和服务能在可接受时间范围内恢复并达到可运营状态。应将这些努力视为灾难性停机的最后手段，因为执行这种切换以及恢复正常服务所需的时间、资金和资源可能极其昂贵。

## 1.5　本章小结

第 1 章主要介绍获取 CCSP 认证证书的要求，并概述包含考试内容的六大知识域。还简要介绍一些基础安全概念，这些基础安全概念是随后开展深入、全面讨论的基石。