cloud security alliance

Certificate of Cloud Security Knowledge (CCSK) 云安全知识认证 V4

获全球卓越奖的专业认证金奖，是唯一获此殊荣的专业认证。

获网络防御全球奖，在全球75个IT技术认证薪酬和热门度排行榜前三，网络安全认证领域名列第一

CCSK是“云计算安全认证之母”，中立权威的国际云安全知识证书，并认证关键云安全领域的能力。

—CIO.com, Top Ten Cloud Computing Certifications

https://c-csa.cn/training/course/

CCSK™ Certificate of Cloud Security Knowledge

认证机构

国际云安全联盟

Cloud Security Alliance (CSA)

国际云安全联盟（CSA）创立于2009年，作为世界领先的独立、权威国际产业组织，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识和全面发展，在全球范围内与其他国际组织机构、政府、高校、企业开展深入而广泛的合作中，以其中立性、敏捷性和专业性被各界认可，是云计算领域的 “ISO”、“ITU”国际标准组织。

云安全联盟大中华区（CSA GCR）作为CSA全球四大区之一（其它大区为美洲区、亚太区、欧非区），是在中国工信部、公安部、网信办支持下首家注册备案的国际非营利组织。**CSA GCR立足于中国，作为国际桥梁联接世界，致力于构建国际数字安全的生态体系。**

CSA组织行业协会、政府、企业及其从业者和个人成员的专业知识，提供特定于云安全和下一代数字技术安全的研究、教育、认证、活动。通过CSA平台，使CSA成员及社区所有成员各方可以共同工作，相互受益。

4大区运营实体

100+分支机构

18万+个人会员

2500+企业会员

80+研究工作组

6000+研究专家

2009 CSA正式成立，发布了全球首个全面的云安全最佳实践**《云计算关键领域安全指南》**

2010 发布云安全领域黄金标准**云控制矩阵CCM**，推出云计算安全知识认证CCSK

2011 欧盟、美国**云计算战略**在CSA峰会上发布

2013 推出全球权威云安全评估认证**CSA STAR**

2015 在中国推出**CSA C-STAR认证**

2017 发布云安全系统认证专家**CCSSP**

2019 推出CSA **GDPR首席认证审计师**课程，受欧盟国家认可

2020 发布零信任认证专家**CZTP**，推出针对企业的GDPR合规自检和第三方认证

2021 发布数据安全认证专家**CDSP**，以及区块链专业人员认证**CBP**

2022 发布认证数据保护官**CDPO**

2023 发布云渗透测试认证专家**CCPTP**，并更新零信任认证专家**CZTP2.0**

2024 更新数据安全认证专家**CDSP2.0**

数据安全认证专家

课程介绍

CCSK（Certificate of Cloud Security Knowledge）云安全知识认证，是国际权威组织云安全联盟于2011年发布的培训和认证计划，是云计算行业面向个人用户的全球首个安全认证。通过CCSK的考试测试了关于云安全广泛知识基础，确保与云计算相关的从业人员对云安全架构、云安全威胁和云安全最佳实践有一个全面的了解和广泛的认知，帮助安全专业人员深入了解云安全，并为解决云安全问题提供帮助。

课程目标

- 了解云计算对治理、法律、风险和法规遵从的影响。
- 学习适应云部署的现有安全原则和实践，包括云对所有传统安全域的影响。
- 能够将云计算关键领域安全指南、云控制矩阵等研究成果实际应用到云安全项目中。
- 顺利通过CCSK笔试并获得证书。了解云模型和架构，以及如何应用共享责任模型构建云安全项目。

课程对象

IT审计员，IT 专业人士，云安全从业人员，网络安全从业人员及在校学生等，需基本了解各种网络安全、云计算的相关概念，及具有一定的安全基础，包括了解防火墙、身份管理和安全发展等安全的专业知识。

课程价值

- **能力证明**：证明持证人员在云安全关键问题上的能力。
- **就业机会增加**：填补云计算认证专业人员的技能缺口来增加就业机会。
- **能力提升**：培养全球公认标准的云安全知识体系，包括技术知识、技能和能力，更好使用云安全控件；通过处理从云治理到配置技术安全控制的广泛职责，学习建立安全最佳实践的基线。
- **持续学习**：获取宝贵的职业提升资源，包括交流想法、工具和与同龄人建立联系，并且在国际社区中持续学习。

CCSK®
Certificate of
Cloud Security Knowledge

课程大纲

本课程分为6个模块，涵盖CSA指导的14个领域,涵盖了云计算的架构、治理、合规、操作、加密和虚拟化等内容。知识体系内容包括CSA的《云计算关键领域安全指南》、《云控制矩阵》（CCM）、《云计算： 信息安全收益、风险和建议》

模块1-云架构

- 1.1 云计算简介
- 1.2 云架构简介
- 1.3 云的基本特征
- 1.4云服务模型
- 1.5 云部署模型

模块2-云基础设施安全

- 2.1 云计算基础设施安全
- 2.2 保护虚拟网络
- 2.3 保护计算工作负载
- 2.4 管理平面安全
- 2.5 业务连续性/灾难性恢复

模块3-管理云安全和风险

- 3.1 风险与治理
- 3.2 法律
- 3.3 合规与审计

模块4-云数据安全

- 4.1 云数据存储
- 4.2 保护云中的数据
- 4.3 其他数据安全选项
- 4.4 数据安全生命周期

模块5:-保护云应用程序、用户和相关技术

- 5.1 应用安全
- 5.2 身份和访问管理
- 5.3 相关技术介绍

模块6-云安全操作

- 选择云提供商
- 安全即服务
- 事件响应

考试与认证培训

- **培训标准课时：** 16小时
- **培训与考试认证费用：**6980元/人（其中：培训费用4500元/人；考试认证费2480元/人）。
- **考试要求：**CCSK 是限时考试，题型为单选题和判断题，共60道题，必须在90分钟内完成.，80%以上的成绩才能通过考试。
- **考试入口：**https://exam.c-csa.cn.

CCSK 证书

CCSK®
Certificate of
Cloud Security Knowledge

哪些企业/人员学习CCSK

- **云提供商和信息安全服务公司。**希望展示在云技术方面的专业知识作为竞争优势，因此鼓励其员工从一开始就获得CCSK。能够声明他们的员工持有CCSK可以让他们的潜在客户放心，因为企业知道必要的技能不仅能在他们的项目中发挥作用，还可以通过培养的人才整体提升企业在云安全业务的能力。

- **云客户。**面临越来越多的云提供商和服务，以及相应的风险和收益。与许多不同的云提供商打交道的企业用户发现，CCSK特别有助于建立安全最佳实践的基线，因为他们需要处理广泛的责任，从云治理到配置技术安全控制。

- **第三方评估机构。**CSA STAR/C-STAR，及中国政府、美国政府等关于云计算的第三方评估机构都有CCSK，因为它们需要客观、一致的云安全知识水平和良好实践的掌握。

- **提供审计、认证或认证服务的个人和公司。**随着越来越多的系统迁移到云计算，他们需要通过全球公认的认证、云的专业知识和特定于云的安全保证，来提升他们的审计能力及给客户信心。

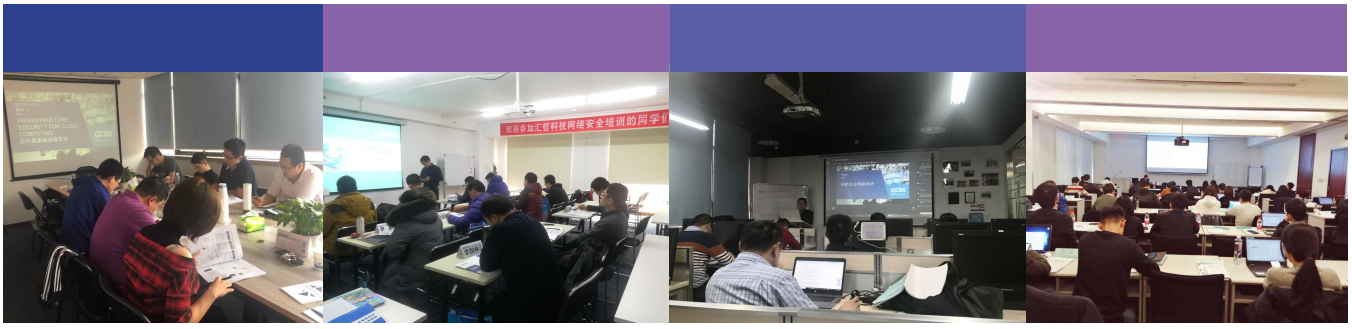
- **个人对象。**对于云计算、网络安全和信息安全相关管理岗位、技术开发人员，运维人员等云安全从业人员；IT审计员，IT 专业人士，网络安全从业人员及具有云计算及网络安全基础的在校学生等都是使用的。

学习基础：基本了解各种网络安全、云计算的相关概念，具有一定的网络工程或安全基础更好。

谁已获得了CCSK证书?

CCSK持证者已超过70000人。在中国，获得CCSK证书的学员覆盖1000多家企业机构，包括政府、教育机构、安全企业，行业用户等，如：公安一所、公安三所、复旦大学、清华大学、中国电信、中国移动、联通、中国银行、工商银行、平安银行、华为、腾讯、360、奇安信、深信服、上汽乘用车、IBM、德勤、绿盟、启明星辰、天融信、浪潮、惠普、安恒信息、中国一汽、恒大集团、海尔集团等单位。

CCSK持证者一般从事以下工作：信息安全总监、CISO、网络安全工程师，安全顾问，云安全治理工程师，安全架构师，高级安全工程师、安全总监、安全运维、技术售前等。



CCSK®
Certificate of
Cloud Security Knowledge

CCSK考试关键概念

附录A：CSA云计算关键领域安全指南第4版

域1-云计算概念与架构

1.1 定义云计算

- 服务模型
- 部署模型
- 参考架构模型
- 逻辑模型

1.2 云安全范围，责任和模型

1,3 云安全关键领域

域2-治理与企业风险管理

2.1 云治理工具

2.2 云中的企业风险管理

2.3 各种服务模型和部署模型的影响

2.4 云风险衡量工具

域3-法律问题、合同和电子发现

3.1 数据与隐私保护治理的法律框架

- 跨境数据传输
- 区域考虑

3.2 合同和供应商选择

- 合同
- 尽职调查
- 第三方审计与认证

3.3 电子发现

- 数据保管

域4-合规与审计管理

4.1 云合规

- 合规对云合同的影响
- 合规范围
- 合规需求分析云

4.2 审计管理

- 审计权
- 审计范围
- 审计要求

域5-信息治理

5.1 治理领域

5.2 数据安全生命周期的六个阶段及其关键要素

5.3 数据安全功能、参与者和控制

域6-管理平面和业务连续性

6.1 云业务连续性与灾难恢复

6.2 防失效架构

6.3 管理平面安全

域7-基础设施安全

7.1 云网络虚拟化

7.2 云网络安全变更

7.3 虚拟设备的挑战

7.4 软件定义网络（SDN）安全效益

7.5 微分隔和软件定义边界

7.6 混合云要考虑的事项

7.7 云计算和工作负载安全性

域8-模拟化和容器

8.1 主要虚拟化类别

8.2 网络

8.3 存储

8.4 容器

域9-事件响应

9.1 事件响应生命周期

9.2 云对事件响应的影响

域10-应用安全

10.1 事件响应生命周期

10.2 云对事件响应的影响

域11-数据安全和加密

11.1 数据安全控制

11.2 云数据存储类型

11.3 对迁移到云数据的管理

11.4 云数据安全

域12-身份、权限和访问管理

12.1 云计算IAM标准

12.2 管理用户和身份

12.3 认证和凭证

12.4 权限和访问管理

域13-安全即服务

13.1 安全即服务潜在的收益和关注点

13.2 安全即服务的主要类别

域14-相关技术

14.1 大数据

14.2 物联网

14.4 移动互联网

14.5 无服务器计算

CCSK
Certificate of
Cloud Security Knowledge

CCSK考试关键概念

附录B：云安全联盟-云控制矩阵

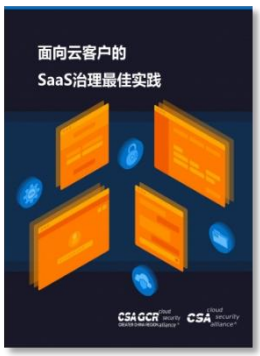
- CCM 域
- CCM 控制项
- 架构相关
- 交付模型适用性
- 适用性范围
- 标准和框架映射

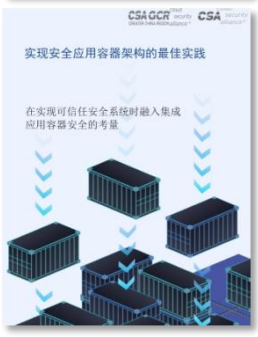
附录C：ENISA云计算：信息安全收益、风险和建议

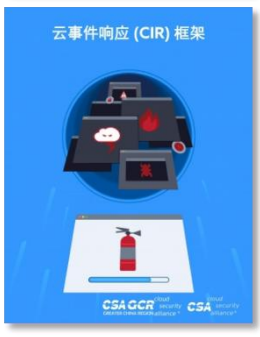
- 隔离失效
- 经济的拒绝服务
- 许可风险
- 虚机跳跃
- 所有场景中常见的五个关键法律问题
- ENISA研究中的排名靠前的风险
- 虚拟开放格式OVF
- 治理缺失的潜在漏洞
- 用户配置漏洞
- 获得云服务提供商的风险问题
- 云安全的收益
- 风险 R.1 – R.35 和潜在的漏洞
- 数据控制器与数据处理器的定义
- 在IaaS模型中, 谁负责客户系统的监控

学习材料

CSA报告《CSA 云安全指南 v4》、《云控制矩阵CCM 3.0.1》、ENISA 报告《云计算： 信息安全收益、风险和建议》、《云计算的11类顶级威胁》、《云安全现状、挑战和安全事件》等。







学习材料下载入口: https://c-csa.cn/research/results/i-4/

CSA GCR

官网：https://c-csa.cn
邮箱：info@c-csa.cn
电话：19925407556