Study Guide

Exam Review and Tips for CCSP®

# Checklist of Exam Objectives: Areas to Study

If you are taking the exam before August 2022, you should utilize the CCSP outline dated August 2019 to prepare for the exam.

<https://www.isc2.org/Certifications/CCSP/Certification-Exam-Outline>

If you are taking the exam after August 2022, you should utilize the CCSP outline dated August 2022 to prepare for the exam.

<https://www.isc2.org/-/media/ISC2/Certifications/Exam-Outlines/CCSP-Exam-Outline-2022.ashx>

Use the free flashcards to help assess your understanding and the study guides' assessment questions that accompany the CCSP certification path courses.

<https://cloud.connect.isc2.org/ccsp-flashcards>

# What you need to know

CCSP Examination Information

|  |  |
| --- | --- |
| **Length of exam** | 3 hours |
| **Number of items** | 125 |
| **Item format** | Multiple choice |
| **Passing grade** | 700 out of 1000 points |
| **Exam language availability** | English and Japanese |
| **Testing center** | Pearson VUE Testing Center |

# How to prepare

Be sure to prepare by knowing the exam outline in the following ways:  
1.) Definitions  
2.) Characteristics  
3.) Integrating concepts across domains  
  
Guidelines for approaching questions on the exam:

A big answer encompasses a smaller solution and is correct if it is a general question. Specific questions need specific answers and not general ones.  
Don't choose variables or exceptions that are correct answers with the word “if.” Choose the standard. Don't supply a definition for the request of characteristic and vice versa.  
Don’t the specific implementation unless you are asked for such. Take a manager’s perspective before that of a technician. Training is key to resolving what may appear as a technical problem. Always apply administrative (non-technical) controls before technical. Examples of administrative controls are awareness, training, directives, and policy. Sr management is ultimately accountable for security, but security is everyone’s responsibility.

**TERMS AND DEFINITIONS**

**Authenticated Encryption with associated data (AEAD):** Symmetric encryption algorithms simultaneously support and apply confidentiality and authentication.

**Blue/green**: May be used where the organization has a mirror of the production environment and the logic that can switch users to the new environment once the functionality confidence is reached.

**Container**: Small form factor-independent executable package of software that is installed and maintained upon a host operating system and includes everything that is needed to run an application, which provides for system tools, libraries, settings, and code.

**Continuous integration/continuous delivery (CI/CD):** An integrated set of practices and tools to merge developer code, build and test software, and develop deploy-ready packaging.

**Domain Keys Identified Mail (DKIM):**

An asymmetric cryptographic key system that creates organizational nonrepudiation of messaging. Emails are received through proof-of-origin processing to detect spoofing and other fraudulent behavior.

**DNS shadowing**: Threat where the attacker gets access to the domain registrant’s account and creates subdomains from the parent domain of the victim to draw unsuspecting visitors to bogus sites.

**Domain-based Message Authentication, Reporting, and Conformance (DMARC):**

A scalable system provides policy configuration for message validation, disposition, and reporting that mail-sending organizations can use for email lifecycle management.

**Forward secrecy**: Also known as perfect forward secrecy, forward secrecy is the cryptographic

protection for encrypted data based upon the discovery or compromise of a private key in an asymmetric pair. The session key used in a previous session will not be available for decryption.

**Immutable**: New virtual systems based on a validated and version-controlled image. When a new system is required, the old is destroyed after the new is deployed.

**Information security continuous monitoring (ISCM) NIST 800-137:** defines Information security continuous monitoring (ISCM) as “maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.”

**Security Content Automation Protocol (SCAP):** SCAP is a multi-purpose framework of specifications that supports automated configuration, vulnerability and patch checking, technical control compliance activities, and security measurement. Goals for the development of SCAP include standardizing system security management, promoting interoperability of security products, and fostering the use of standard expressions of security content.

**Security Operations Management System (SOMS) ISO/IEC 18788-2015, Management systems**

**for private security operations** — Requirements with guidance for use are designed for organizations conducting or contracting security operations. The document provides a business and risk management framework for the effective conduct of security operations.

**Sender Policy Framework (SPF):** Email authentication defines a process to validate an email message sent from an authorized mail server to detect forgery and prevent spam. The domain owner can identify exactly which mail servers they can send from with SPF protocols.

**Simple Network Management Protocol (SNMP):** SNMP is an internet-standard protocol for collecting and organizing information about managed devices on IP networks. It can determine the “health” of networking devices, including routers, switches, servers, workstations, printers, and modem racks.

**Virtual Extensible LAN (VXLAN):** Encapsulates layer two frames within layer 4 UDP packets, using techniques like a VLAN but supporting up to 16 million logical networks.

**SAMPLE QUESTIONS**

1. **A security group maintains IP and port address filtering. The main attributes of filtering are:**
2. Ingress, egress, and descriptions
3. Ingress, inbound, and outbound
4. Egress, ingress, and outbound
5. Outbound, inbound, and afterward
6. **Your security team needs to protect instances launched on your cloud Infrastructure-as-a-Service from being accessed by external IP addresses that don’t originate from company resources. To facilitate this requirement, what should you do?**
7. Configure a security group that has an ingress rule that only allows access from approved resources
8. Configure a security group that has an egress rule that only allows access to approved resources
9. Configure a firewall that has an egress rule that only allows access to approved resources
10. Configure a firewall that has an ingress rule that only allows access from approved resources
11. **You’ve created a virtual private cloud (VPC) and have launched an instance from your cloud management console. You are trying to connect to the instance from the Internet with SSH. You get an error that tells you that you cannot connect. When you look at the host address for your SSH session, it states that it is 10.1.1.1. What is the problem?**
12. You’re attempting to use a private IP address
13. The security group is blocking access
14. The company firewall is blocking access
15. This error always happens with the initial connection attempt
16. **Your organization is transitioning from a data center capital expenditure model to a cloud operational expenditure model. You are responsible for maintaining and provisioning the cloud services that the cloud application developers consume in your company. You find that the virtual machines' patching, maintenance, and updating take up time that slows down the development of cloud applications. The primary mandate is to get the applications built and distributed as quickly as possible. What would you recommend for the developers to use?**
17. Function-as-a-Service
18. Traditional data center service
19. High-speed virtual machines
20. Load-balancing
21. **If an organization is measuring its maturity for incident management in the cloud, at what phase would they establish core processes and tools?**
22. Prepare
23. Detect
24. Respond
25. Sustain

​

1. **Before consuming cloud services,​ the change management process in an organization was intermittently successful at communicating necessary changes to the business in a way they understand. Now that they are using the cloud to satisfy most of their business needs, little has changed in the convoluted explanations of necessary change, except that the changes are now more rapid. What is most likely the problem?​**
2. The IT team is focused on technology and not services.
3. The IT team should embrace DevSecOps
4. The IT team should slow down.
5. The business should learn more about technology
6. An organization has struggled in the past with shadow-IT issues where department heads would assess their own needs and acquire their technology without getting professional input from the IT department. Now that they are consuming cloud services, the same practices are made more accessible by using a credit card. What would you suggest to them to track the trend to make regular assessments of the issue?
7. An ISCM strategy along with the provider cloud monitoring tool
8. An ISCM approach along with a log monitoring tool
9. An ISCM strategy along with host intrusion prevention systems
10. st checks in on the reduction of Shadow IT periodically
11. An organization has recently discovered that they’ve been compromised by an APT resident on their cloud compute and storage systems for nine months. When they investigated, they found that the data combined from multiple systems and services formed a cyber kill-chain that presented numerous opportunities to prevent the APT's successful inhabitation. The main problem is that the evidence was spread among the multiple systems and services. What would you recommend to avoid this inhabitation in the future?
12. Security information and event management
13. Layer four firewall
14. Layer seven firewall
15. Intrusion detection system
16. Name three elements that should be reflected in a management system for private security operations.
17. Risk management, continuous improvement, human rights.
18. Risk management, continuous improvement, current technology
19. Risk management, continuous improvement, current rollout schedule
20. Risk management, leadership commitment, current technology
21. Name two issues that are part of broader concerns related to the security of event logs.
22. Log rotation and synchronized time
23. Reconfiguration and logs monitor
24. Logs monitor and log rotation
25. Synchronized time and distributed systems

**ANSWERS**

1. B. The basic behavior of a security group is a layer four firewall; allow/deny ports/IPs ingress/egress
2. A. They need to configure a security group that has an ingress rule that only allows access from approved resources
3. A. The address you are using cannot be accessed outside of your virtual network
4. A. FaaS bypasses the need to maintain and update operating systems in an IaaS model.
5. A. Prepare is when the organization would choose the processes and tools for measuring incident management maturity
6. A. The IT team is focused on technology and not services.
7. A. An ISCM strategy along with the provider cloud monitoring tool
8. A. Security information and event management
9. A. Risk management, continuous improvement, human rights.
10. A. Log rotation and synchronized time