Certified Cloud Security Professional

Study Guide

Table of Contents

Certified Cloud Security Professional Certification & Exam

CCSP Certification Requirements

The CCSP exam requires a candidate to possess a minimum of five (5) years cumulative paid work experience in the information technology industry. Three (3) years must be in information security and one (1) year in one (1) or more of the six (6) CCSP CBK's domains. Moreover, obtaining (ISC) ²'s CISSP credential can be substituted for the CCSP's recommended experience. If a candidate does not have the recommended experience for CCSP, then they will be eligible to become an Associate of (ISC) ² once they have passed the CCSP exam. After passing the exam, the (ISC) ²'s Associate will have six (6) years to acquire five (5) years recommended experience.

Register for the CCSP Exam

You need to perform a number of steps to book your CCSP exam at Pearson VUE website. The Pearson VUE conducts innovative computer-based testing solutions through a secure and electronic test delivery.

- Review exam availability by credential
- Visiting the Pearson VUE website
- Create a Pearson VUE account and then review the Pearson VUE NDA
- Select an appropriate testing center
- Select a convenient time
- Pay for the exam
- Check the confirmation through E-mail that the Pearson VUE will send to you. This E-mail includes appointment details, testing location, and all other relevant instructions.

CCSP Exam Cost

The CCSP Exam price varies according to the locations. Please refer to the following table for price details of different countries.

CCSP Country	Price for the exam
United States	$599
Asia Pacific	$599
United Kingdom	GBP 479
Middle East	$599
Africa	$599

CCSP Exam Format

Number of Questions	**125**
Length of the examination	4 hours
Type of Questions	Multiple Choice
Passing grade	700 points out of 1000 points
Language	English
Testing Center	Pearson VUE

The CCSP CBK and Exam Weights

The CCSP CBK includes the topics, material, or objectives that define every aspect of cloud security. It consists of following six (6) domains:

Domain Name	Percentage of the Exam
Architectural Concepts and Design Requirements	19%
Cloud Data Security	20%
Cloud Platform and Infrastructure Security	19%
Cloud Applications Security	15%
Operations	15%
Legal and Compliance	12%
Total	100%

Core Concepts of the CCSP Exam

The core concepts for CCSP exam include:

- Architectural Concepts
- Design Requirements
- Data Classification
- Cloud Data Security
- Security in the Cloud
- Responsibilities in the Cloud
- Cloud Application Security
- Operations Elements

- Operations Management
- Legal and Compliance

Architectural Concepts

The key topics to architectural concepts are described below.

Understand business requirements: All management decisions, including the risk and security-related decisions, are driven by the business needs. The management must consider security and risks before these decisions are made and they should not take precedence over the operational requirements of the enterprises.

Describe cloud service models: You must understand three cloud service models that include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) and the difference among one another.

Understand cloud deployment models: For CCSP exam, the candidate must understand the properties of each of the four deployment models that include Private, Public, Hybrid, and Community. Knowing their difference is also essential.

Cloud Design Requirements

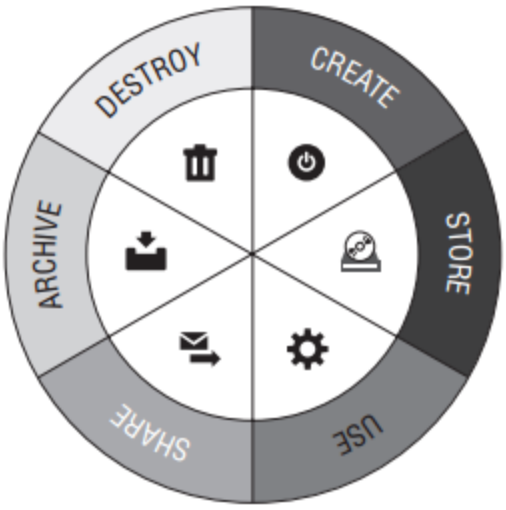
Apart from architectural requirements, the candidate should also learn design requirements for the cloud. The candidate needs to know about various inputs for the security decisions and the business activities to determine the requirements, such as:

How to determine business requirements: The CCSP candidate should understand the functions of business impact analysis and how it allows the enterprises to ascertain the value, inventory, and vitality of corporate assets.

Be familiar with boundaries of each cloud service model: The candidate should know which model can assign typical control and dependence to the groups involved in the cloud relationship.

Role of cloud architecture and design for supporting data security: The students must understand how hardening devices work, how encryption schemes can be applied, and how in-depth

FIGURE 1 Data life cycle



defense improves the protection of data and thwarts potential cybersecurity threats to the cloud.

Data Classification

In this section, the CCSP candidates would learn how data is classified and categorized, why the site of data matters, what are the best data practices and concepts and knowing about data retention policy and deletion/disposal/eraser requirements.

Different forms of data analytics: The candidates should know about data mining, its real-time analytics, and about agile business intelligence that involves recursive and iterative tools to identify trends in trends, and detect more oblique patterns in recent and historical data.

The Data lifecycle: Figure 1 below demonstrates the important phases of data lifecycle that include how to create, store, use, share, archive, and destroy data.

Data Categorization*:* Usually, the data owner undertakes the responsibility to categorize data. The enterprises should consider some elements when performing data categorization, such as regulatory compliance, business functions, and functional units. The regulatory compliance is the process of complying with one or more of the acts that might include Health Insurance Portability and Accountability Act, Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and Graham-Leach-Bliley Act.

Data classification: Like data categorization, data classification is indeed a responsibility of the data owner. It's done during the Create Phase. Data classification involves several types that include sensitivity, jurisdiction, and criticality.

Data Labeling: Once the data has been categorized and classified, it should be properly labeled in order to indicate the data ownership, data type, name, nomenclature, and so on. Data labeling can also involve following types of information.

- Data of data creation
- Date of data scheduled disposal/destruction
- Data confidentiality level
- Data handling directions
- Data distribution instructions
- Data access limitations
- Data source and jurisdiction

Intellectual property protection: This involves the protection of trade secrets, patents, copyrights, and trademarks.

Data retention policy: It defines how long the data will be retained in the organization. Besides, data retention also ensures the protection of retained data. The data should not be changed or manipulated.

Data disposal: Data disposal is the process of discarding or erasing data because its purpose has been achieved or it has been no longer useful for the organization.

Cloud Data Security

When the data is transferred over the network, its confidentiality, integrity, and availability (also known as CIA triad) must be protected and ensured. Doing so requires the security professionals to take some proactive measures that are described below.

Understand cloud storage architectures: There are numerous ways to store data in the cloud and each way has different cost and advantages. These ways include file-based storage and block storage, object-based storage, databases, and content delivery network (CDN).

Cloud data security foundational strategies: Various effective strategies are available today to ensure cloud data security. For example, encryption is the best technique in this regard. It can be either symmetric or asymmetric. When the sender sends data using encryption scheme, he/she will encrypt the data or plain text into the unreadable form, called ciphertext. The recipient will decrypt the data by using the key provided by the sender. In addition to encryption, other techniques include key management and Homomorphic encryption.

SIEM Technology: The candidates should understand the purpose of SIEM implementation and the issues and challenges associated with this solution.

Egress Monitoring: It's also known as DLP which can stand for any combination of the terms such as data protection, prevention, leak, and loss. Egress monitoring is the process of examining data as it leaves the production facility. Egress monitoring is used to provide additional security, policy enforcement, enhanced monitoring, and regulatory compliance.

Security in the Cloud

In this section, the candidates would learn the distinct and shared responsibilities of the cloud service provider and customer in terms of managing BC/DR activities as well as risks. The candidates would also learn the potential risks to cloud computing platforms and their safeguards and countermeasures.

Shared cloud platform risks and responsibilities: Since both service provider and the customer are parties to the processing of data, therefore, they will have shared risks and responsibilities associated with that data. Both parties should sign a contract to codify these risks and responsibilities. Also, the service provider must protect the PII (personally identifiable information) of the customers.

Cloud computing risks by service and deployment model: The cloud service models include IaaS, PaaS, and SaaS, and cloud deployment models involve private, community, public, and hybrid model. Each service model and deployment model can be vulnerable to various threats. For example, the risks associated with private cloud might include personal threats (inadvertent and malicious threats), natural disasters, external threats (such as eavesdropping, DoS/DDoS, and so on), regulatory noncompliance, and malware attacks.

Virtualization: In computing, virtualization is the act of creating a virtual representation of something, rather than a physical one. Virtualization can be applied to a single host, network, storage devices, servers, and applications. The purpose of virtualization is to reduce costs and boosts efficiency. There are various types of threats associated with the virtualization technology. For example, the malicious parties launch attacks on Hypervisor, a software that operates virtual machines.

Disaster Recovery (DR) and Business Continuity Management (BCM): The candidates must understand the basic concepts associated with DR and BCM. These topics include Cloud-Specific BIA concerns, customer and provider shared BC/DR responsibilities, declaration of disaster events, and failover testing.

Cloud Responsibilities

In this section, the CCSP candidates would learn the responsibilities of the parties, the service provider, and the customer.

Foundations of Managed Services: Both the cloud vendor and the cloud customer have different needs. The cloud providers maximize profits whereas the customers need the cheapest and reliable services. In order to avoid further complications, both parties should sign the Service Level Agreement (SLA) whose purpose is to bind both parties on negotiated terms.

Business Requirements: The business requirements in cloud provider perspective include the provision of the datacenter from which the provider will provide reliable services to its customers. The provider should ensure the security of datacenter's hardware components, manage hardware

configuration, set hardware to log events and incidents, determine computational components, and configure secure remote administrative access. Besides, the provider should also ensure the protection of logical framework that includes installation of virtual OSs and configuration of various other virtualized components. Moreover, the provider should also ensure the security of networking through firewalls, IDS/IPS, and honeypots. Communication protection can be ensured by using encryption, Virtual Private Networks (VPNs), and strong authentication.

Responsibilities in each cloud service model*:* Both parties must know what responsibilities each of them has about the configuration of SaaS, PaaS, and IaaS.

Types of Audit Reports*:* The candidate should understand the difference among SOC 1, 2, and 3 reports and the Type 1 and 2 of SOC 2, and the SOC 3.

Cloud Application Security

This section describes application testing and validation in order to ensure that the cloud applications are secure and protected.

Components of the STRIDE threat model: The STRIDE threat model involves the six threat categories, such as:

- Spoofing
- Repudiation
- Tampering
- Denial of Service
- Information disclosure
- Elevation of privilege

Stages of the SDLC: The CCSP candidates should understand the stages in the SDLC model. These stages are listed below.

- Defining
- Designing
- Developing
- Testing
- Secure Operations
- Disposal

Identify and Access management: Identity and Access Management (IAM) has a crucial role in managing users. IAM provides role-based access to the users and prevents unauthorized access. It also ensures the right access to right resources at right time to right individuals.

Operations Elements

In this section, the candidate will be learning the review of cloud provider's datacenter.

Redundancy in the design of cloud datacenters: The CCSP candidate should understand how to implement the redundancy in the design of the cloud datacenter. The candidates also know that the redundancy for infrastructure, systems, and all other components are essential. Redundancy includes utilities (water, power, and connectivity), data storage, processing capabilities, personnel, and contingency and emergency services.

Four tiers of datacenter redundancy: The CCSP candidates must know the four tiers of datacenter redundancy that is published by the Uptime Institute.

Training and awareness*:* It is imperative to know how training and awareness impact the risks of the enterprise, which element best support training efforts.

Difference DAST and SAST: The candidates should also understand "which is black-box testing," "which is white-box testing," "which includes reviews of source code," and "which is carried out in runtime."

Legal and Compliance Procedures

Legal and compliance procedures involve laws and regulations, standards that the CCSP candidates should understand. Some of the standards include ISO, IEC, PCI, GLBA, and HIPAA.

Understand ISO 27001: ISO is not a law but is designed by numerous IT experts across the world. ISO 27001 is a specification for an Information Security Management System (ISMS). ISMS deal with the risk management processes of enterprises.

Understand U.S security and privacy standards, laws, and regulations: These legal acts include GLBA, SOX, HIPAA, and PCI.

Understand the issues related to e-Discovery: This involves the forensic evidence (or digital evidence), chain of custody, and the issues encountering during the forensic acquisition in a cloud environment.

Understand audit process: The audit in the organization is performed to check whether all the resources and services are working accurately and effectively. Besides, audits are carried out periodically.

Understand PII: Personally Identifiable Information (PII) is associated with each employee working in the organization. For example, the PII include the name, date of birth, address, and so on. The PII is often used to trace the employees in large enterprises.

Exam Questions for Practice

1. As being the security analysts in an enterprise, you are asked by the top management to provide a storage solution to the customers so that they can store their data on the cloud, rather than on local physical disks, such as tape or hard drive. What type of solution should you recommend?

A. Masking
B. Removable hard drives
C. Cloud backup solutions
D. Online backups

Correct Answer is C – You should provide cloud backup solution to the customers so that they can store their data using a storing service through the internet. Remaining options are irrelevant. For example, Masking technology is used to partially conceal confidential data.

2. The use of an Infrastructure as a Service (IaaS) solution can provide several benefits to the customers, such as:

A. Transfer of ownership cost
B. Energy and cooling efficiencies
C. Metered service
D. Scalability

Correct Answer is A – Transfer of ownership cost, in fact, is the primary advantage to the customers using IaaS solution. Remaining options such as Energy and cooling efficiencies, Metered service, and Scalability are a part of the advantage of a cloud environment and, hence, they are not primary benefits of IaaS adoption.

3. Identify the correct set of four cloud deployment models?

A. External, Private, Hybrid, and Community
B. Public, Internet, Hybrid, and Community
C. Public, Private, Hybrid, and Community
D. Public, Private, Joint and Community

Correct Answer is C – The correct sequence of four cloud deployment models is Public, Private, Hybrid, and Community. Remaining options are incorrect because of external, internet, and joint are not deployment models.

4. _____is a mathematical code that enables encryption of software/hardware to encode and then decode the encrypted message.

A. Masking
B. Public key
C. Encryption key
D. PKI

Correct Answer is C – In fact, the encryption key is used to encrypt and decrypt the message. First and foremost, the sender encrypts the message using an encryption key. After that, the recipient will decrypt that message using the key provided by the sender.

5. Identify the correct sequence of the STRIDE threat model.

A. Spoofing, Tampering, Nonrepudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
B. Spoofing, Tampering, Repudiation, Information Disclosure, Distributed Denial of Service, and Elevation of Privilege
C. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Social Engineering Elasticity
D. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege

Correct Answer is D – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege is the correct sequence for STRIDE threat model. Remaining sequences are incorrect.

6. IaaS is an abbreviation for:

A. Internet as a Service
B. Infrastructure as a Service
C. Infrastructure as a Security
D. Internet as a Security

Correct Answer is B – In fact, Infrastructure as a Service (IaaS) is the correct abbreviate for IaaS. Remaining options are incorrect.

7. Which of the following is/are the benefit (s) of Virtualization?

A. Minimize downtime
B. Provide resources and applications faster
C. Enable disaster recovery and business continuity
D. Reduce capital and operating costs
E. All of the above mentioned

Correct Answer is B – In fact, all the options are correct because each of them is the potential benefit of virtualization.

8. The company has hired you as a security analyst. The top management recently asked to deploy a solution that makes sure that a particular sender creates and sends item or message to a particular recipient. Which of the following solution would you recommend?

A. Bit splitting
B. Nonrepudiation
C. DLP
D. PKI

Correct Answer is B – Nonrepudiation, in fact, is the assurance that the specific author cannot deny the authenticity of his/her signature on a document or send the item or a message that he/she originated.

9. Encryption keys can be destroyed through:

A. Crypto-shredding
B. Obfuscation
C. PKI
D. Poor key management

Correct Answer is A – Crypto-shredding is the act of destroying the encryption keys. Remaining options are invalid or no longer a relevant.

10. As being the security analyst in an organization. Your task is to replace sensitive data with the unique identification symbols that include all important information regarding data without compromising its security. Which of the following techniques should you apply in this process?

A. Tokenization
B. Obfuscation
C. Elasticity
D. Randomization

Correct Answer is A – In this particular scenario, you need to apply tokenization. In fact, tokenization is the process of replacing sensitive data with the unique identification symbols that include all important information regarding data without compromising its security.

11. Your company needs to implement a Platform as a Service (PaaS) deployment model. The top management has hired you for this purpose. Which of the following data storage types should you use with PaaS model?

A. Raw and block
B. Tabular
C. SaaS application
D. Databases and Big Data

Correct Answer is D – In this particular scenario, you need to use databases and big data storage types. The remaining options are irrelevant.

12. _____ is the software technology that encloses application software from the underlying OS on which it's executed.

A. SaaS
B. VMware
C. Application virtualization
D. Hypervisor

Correct Answer is C – Application virtualization encloses application software from the underlying OS on which it's executed. The remaining options are irrelevant. SaaS is a deployment model. VMware and Hypervisors are also not used for this purpose.

13. You have been hired as a legal expert or attorney in the enterprise. The top management of your company asked you to enact legislation in order to protect public and the shareholders from enterprise fraudulent practices and accounting errors. Which of the following legislation should you use in this particular scenario?

A. HIPAA
B. Sarbanes-Oxley Act (SOX)
C. Gramm-Leach-Bliley Act (GLBA)
D. PCI

Correct Answer is B –Sarbanes-Oxley Act (SOX) is the legislation that you should use to protect in order to protect public and the shareholders from enterprise fraudulent practices and accounting errors. This legislation, in fact, was enacted in response to the accounting scandal that was a cause of Enron's bankruptcy. The remaining options are irrelevant.

14. _____ cloud infrastructure is used by the general public and is owned, operated, and managed by an academic, business, and government agencies.

A. Personal cloud
B. Hybrid cloud
C. Public cloud
D. Private cloud

Correct Answer is C – In fact, public cloud computing is the cloud infrastructure that is used by the general public and is owned, operated, and managed by an academic, business, and government agencies. The remaining options indicate the different types of cloud models.

15. Uptime Institute is split into _____?

A. Four Tiers
B. Five Tiers
C. Six Tiers
D. Seven Tiers

Correct Answer is A – Uptime Institute is split into four tiers. Tier 1 is the simplistic datacenter. Tier 2 datacenter is little more robust then Tier 1. Tier 3 is referred to as "Concurrently Maintainable Site Infrastructure." Lastly, Tier 4: the fault-tolerant "site infrastructure" is the premium datacenter offering. In this tier, each and every system and element of the facility has integral redundancy such that critical operation can survive both unplanned and planned downtime at the loss of any system or component.

16. Which of following attacks is NOT associated with the STRIDE model?

A. Spoofing
B. Trojan
C. Repudiation
D. Information disclosure

Correct Answer is B – Trojan is not associated with STRIDE Model. As a matter of fact, the STRIDE Model includes Tampering in place of Trojan wrongly placed there.

17. Which of following attacks is associated with the STRIDE model?

A. Rijndael
B. Resiliency

C. Redundancy
D. Repudiation

Correct Answer is D – Repudiation is "R" in the STRIDE model. Remaining options are incorrect and inappropriate here.

18. If the user is gaining permissions above his/her authorized level, then which of the following terms relating to STRIDE model is being compromised?

A. Repudiation
B. Information disclosure
C. Denial of Service
D. Escalation of Privilege

Correct Answer is D – Escalation of Privilege is an "E" the STRIDE model. It indicates that the user is gaining permissions above his/her authorized level.

19. _____ uses a set of principles, methods, or rules for assessing risks based on non-numerical levels or categories.

A. SOC 2
B. Hybrid assessment
C. Qualitative assessment
D. Quantitative assessment

Correct Answer is C – A Qualitative assessment uses a set of principles, methods, or rules for assessing risks based on non-numerical levels or categories. On the other hand, quantities assessment uses a mathematical level or categories.

20. When a conflict of laws takes place, then which of the following determines the jurisdiction in which the dispute should be heard?

A. Criminal law
B. Common law
C. Doctrine of Proper Law
D. Tort law

Correct Answer is C – When a conflict of laws takes place, then the Doctrine of Proper Law determines the jurisdiction in which the dispute should be heard. Tort laws deal with civil liability suits. Common law is used for marriages. Lastly, the criminal laws address the violations of federal or state criminal code.

21. Which of the following types of law deals with civil liabilities suite?

A. Criminal law
B. Common law
C. Doctrine of Proper Law
D. Tort law

Correct Answer is D – Tort laws deal with civil liability suits. Contrarily, the Common law is used for marriages. When a conflict of laws takes place, then the Doctrine of Proper Law determines the jurisdiction in which the dispute should be heard. Lastly, the criminal law addresses the violations of federal or state criminal code.

22. Which of the following types of law deals with deals with the violations of federal or state criminal code?

A. Criminal law
B. Common law
C. Doctrine of Proper Law
D. Tort law

Correct Answer is A – Criminal law deals with the violations of federal or state criminal code. On the contrary, Tort laws deal with civil liability suits. Contrarily, the Common law is used for marriages. When a conflict of laws takes place, then the Doctrine of Proper Law determines the jurisdiction in which the dispute should be heard.

23. _____ is the most essential security consideration when selecting a new computer facility.

A. Utility infrastructure
B. Aircraft flight paths
C. Location adjacent to competitor's facilities
D. Local law enforcement response times

Correct Answer is A – Utility infrastructure is an essential security consideration when selecting a new computer facility. It's important because any datacenter facility should be close to sound facility resources, such as connectivity, water, and power.

24. What is a corporation called who purchases hosting services from a cloud computing provider or cloud server hosting provider and then resells them to its own consumers?

A. VAR
B. Cloud proxy
C. Cloud computing reseller
D. Cloud broker

Correct Answer is C – The cloud computing reseller purchases hosting services from a cloud computing provider or cloud server hosting provider and then resells them to its own consumers.

*****