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**

**Agent of the government**

A private citizen becomes an agent of the government when they perform an act that the government would need a warrant for, such as a search and seizure. Under those circumstances, the citizen must follow the same rules as the government.

**Baselines Minimum requirements**

Especially regarding security as a minimum level.

**Cloud Controls Matrix (CCM)**

Lists and categorizes the domains and controls, along with which elements and components are relevant per the controls. This framework enables cooperation between cloud consumers and cloud providers on demonstrating adequate risk management.

**Conflict of law**

The field of law that resolves the jurisdiction of states or nations with laws that are not in agreement with other states or nations, either domestically or internationally.

**Criminal law**

The body of law that relates to crime. It proscribes conduct perceived as threatening, harmful, or otherwise endangering to the property, health, safety, and moral welfare of people. Most criminal law is established by statute, which is to say that the laws are enacted by a legislature.

**Cross-border transfers**

Multiple laws and regulations restrict or do not allow for information to be transferred across borders or to locations where the level of privacy or data protection is deemed to be weaker than their current requirements.

**CSA Security, Trust Assurance and Risk (STAR) Registry**

The provider will have assessments and certifications that provide differing levels of assurance about the cloud controls they maintain. For instance, some providers have only completed a self-assessment, while others have completed a third-party certification based upon Information

**Security Management System ISO 27001**

Still other organizations have completed a third-party attestation of their cloud controls based upon Service Organization’s System in a SOC 2 Report.

**Data sovereignty**

Implied or explicit right to decide what treatment, care, or disposition (embargo or movement) a nation or state can determine on data by means of its laws.

**Doctrine of plain view**

In some U.S. states, a law enforcement officer may seize evidence without a search warrant if they can see it without making entry to where the evidence resides. This applies in digital forensic searches because it is necessary to perform various kinds of searches on digital evidence that may reveal evidence of a crime not noted in the warrant.

**Due care**

“Due care” is a standard of behavior grounded in the concept of “reasonableness.” Did the actor exhibit a standard of behavior that is deemed by the law to be “reasonable,” i.e., would other individuals in the actor’s position act in a similar manner exhibiting an expected standard of due care?

**Due diligence**

“Due diligence” is not a standard, but rather a mode of conduct. Did the actor do what is appropriate, reasonable, and expected in engaging in a certain activity?

**European Economic Area (EEA)**

The EEA includes EU countries and also Iceland, Liechtenstein, and Norway. It allows them to be part of the EU’s single market. Switzerland is neither an EU nor EEA member, but is part of the single market— this means Swiss nationals have the same rights to live and work in the UK as other EEA nationals.

**European Union (EU)**

An economic and political union of 28 countries. It operates an internal (or single) market that allows free movement of goods, capital, services and people between member states.

As of March 2019 these countries include: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the UK.

**E-discovery**

Electronic discovery (also called e-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

**EU Data Protection Directive 95/46 EC**

Directive 95/46 EC focuses on the protection of individuals regarding the processing of personal data and on the free movement of such data.

**EU General Data Protection Regulation 2016**

Introduces many significant changes for data processors and controllers. The following

may be considered some of the more significant changes: the concept of consent, transfers abroad, the right to be forgotten, establishment of the role of the “data protection officer,” access requests, home state regulation, and increased sanctions.

**Extradition**

Many countries support a formal process whereby one country transfers a suspected or convicted criminal to another country.

**Generally Accepted Privacy Principles (GAPP)**

The AICPA describes 74 privacy principles in detail. These serve as a framework for organizations to use to manage privacy risk.

**Gramm–Leach– Bliley Act (GLBA)**

Also known as the Financial Modernization Act of 1999, GLBA is a federal law enacted

in the United States to control the ways that financial institutions deal with the private

information of individuals. Guidelines Statements that aren’t designed for enforcement, but principles that can assist in accomplishing objectives.

**Harmonization of law**

Specifically, in relation to the European Union, harmonization of law (or simply

“harmonization”) is the process of creating common standards across the internal market.

**Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

Adopts national standards in the United States for electronic health care transactions and national identifiers for providers, health plans, and employers. Protected health information can be stored via cloud computing under HIPAA.

**International law**

The term given to the rules that govern relations between countries.

**ISO/IEC 27017:2015**

This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of cloud-specific information security controls supplementing the guidance in ISO/IEC 27002:2013 and other ISO27k standards.

The “code of practice” provides additional information security controls implementation

advice beyond that provided in ISO/IEC 27002:2013, in the cloud computing context.

**ISO/IEC 27018:2019**

The first international “code of practice” that focuses on protection of personal data

in the cloud. It is based on ISO/IEC information security standard 27002:2013

and provides implementation guidance on ISO/IEC 27002:2013 controls applicable to

public cloud personally identifiable information (PII).

**ISO/IEC 27050 ISO/IEC 27050**

consists of six major components across the discovery phase of a law suit, with an emphasis on the discovery of electronically stored information (ESI).

**ISO/IEC 31000:2018**

A guidance standard not intended for certification purposes, implementing it does not address specific or legal requirements related to risk assessments, risk reviews, and overall risk management.

**Jurisdiction**

The practical authority granted to a legal body to administer justice within a defined area of responsibility.

**Legal hold**

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a legal hold to ensure the preservation of relevant documents.

**NIST SP 800-37r2**

This publication details the NIST Risk Management Framework, a process for managing security and privacy risk. Integrates the Risk Management Framework (RMF) into the system

development lifecycle (SDLC). Provides processes (tasks) for each of the six steps in the RMF at the system level.

**NIST SP 800-53r4**

A standard to ensure that appropriate security requirements and security controls are applied to all U.S. federal government information and information management systems. Policies Guide the overall governance of an organization and require both penalties as well as senior management sponsorship to be effective.

**Privacy Act 1988 The Privacy Act 1988 (Privacy Act)**

is an Australian law that regulates the handling of personal information about individuals. This

includes the collection, use, storage, and disclosure of personal information, and access to and correction of that information. Policy General high-level statement that prescribes actions and consequences for organizational members.

**Procedure**

The methods and instructions on how to maintain or accomplish the directives of the policy.

**Sarbanes–Oxley Act (SOX)**

U.S. legislation was enacted to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise.

**Service Organization Controls 1 (SOC 1)**

Reports on controls at a service organization relevant to user entities’ internal control over financial reporting. Used to provide information to the auditor in order to enable risk assessment.

**Service Organization Controls 2 (SOC 2)**

Reports on controls at a service organization relevant to security, availability, processing

integrity, confidentiality, and privacy. Used to provide management and specified entities with information.

**Service Organization Controls 3 (SOC 3)**

Reports on controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy. Used to provide information for general use by any interested party.

**Standards**

Implementable selections of tools, technology, hardware, and software.

**Subpoena**

The subpoena is deemed issued by an officer of the court and must be obeyed in much the same manner as a warrant.

**Tort law**

A body of rights, obligations, and remedies that sets out reliefs for persons suffering harm because of the wrongful acts of others.

**Trust Services Principles and Criteria (TSP)**

An auditing system whereby various criterion areas are evaluated along with controls within an organization that includes, security, processing integrity, availability, confidentiality, and privacy.

**Warrant**

Authorization issued by a magistrate or other official allows a constable or other officer to search or seize property, arrest a person, or perform some other specified act.

**SAMPLE QUESTIONS**

1. A process that a service organization goes through to provide assurance to their customers that the controls of security meet technical requirements for doing business is called a(n)?
2. Attestation
3. Certification
4. Technical review
5. Management review
6. Your organization is interested in a new cloud service provider as they have a service that you’ve been looking for that more completely fits your business requirements than all of the other providers that you’ve reviewed. While the senior management of your company doesn’t have concerns about their technology controls, they are concerned that the company has only started doing business in the last four months. What type of audit report would most appropriately address this concern?
7. SOC 2
8. SOC 3
9. Trust Services Principle
10. SOC 1
11. An organization is experiencing major problems with shadow IT; namely the individual department heads are each purchasing their own services from cloud providers without going through a central purchasing agent and without getting advice from the technology and security departments. What elements of an Information Security Management System ISMS certification process, like ISO/IEC 27001, would they see most benefit from to help them get control of this dangerous situation?
12. Information Security Policies, Supplier Relationships, Compliance
13. Communications Security, Information Security Policies, Compliance
14. Operations Security, Information Security Policies, Compliance
15. Operations Security, Information Security Policies, Communications Security
16. A controller (an organization consuming service on a cloud providers’ platform and managing personal data of customers) is using data beyond the agreement of when the customer first signed up for the service. In particular the controller is allowing a partner organization to make use of the customer data as a way of performing statistical analysis of a given population set. They have not informed their customers. What element of the *Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds ISO27018:2019* has been violated?
17. Consent
18. Transparency
19. Breach
20. Control
21. What is the minimal documentation that would be provided by a cloud service provider to be in the Cloud Security Alliance STAR registry?
22. Self-assessment
23. Attestation
24. Certification
25. Continuous audit
26. You will be doing business in the European Union (EU). You are concerned about following the guidelines and mandates specified in the regions that make up that union. To select a cloud service provider that most likely aligned with areas affected by EU laws and regulations what should you utilize?
27. ISO/IEC 27001
28. ISO/IEC 27017
29. ISO/IEC 27018
30. StarAudit Framework
31. Your organization wants to verify that the controls that you have applied to the services you are consuming from your cloud provider meet business, regulatory, and best practice requirements. The audit process will most definitely require testing to prove the effectiveness of the con6.trols. What should you do first?
32. Begin the test without delay; it is your right to audit your own system
33. Review the current policy of testing with from cloud provider
34. Never do testing on the providers system
35. Prepare a statement of audit scope
36. What of the following would be the most meaningful area to start in order for an organization to develop a robust risk and compliance environment?
37. Risk management framework
38. Security controls selection
39. Security controls baseline
40. Security controls audit
41. An organization has a set of risks that represent a low likelihood of threats being executed but would have a high impact on critical assets if successfully executed. Since the risks meet the acceptable risk profile and appetite for the organization what may the businesses’ most likely response be to the risks?
42. Modification
43. Avoidance
44. Retention
45. Sharing

**10.** An organization is considering a quantitative analysis of a critical system. It is valued at $9, 600, 000.00. Due to the possibility of a particular disaster, they calculate an exposure factor of 20 percent. What part of the quantitative analysis has been completed.

1. Annual Rate of Occurrence (ARO)
2. Single Loss Expectancy (SLE)
3. Annual Loss Expectancy (ALE)
4. Frequency

**ANSWERS**

1. A. Attestations are designed to provide assurance to their customers that the controls of security meet technical requirements

2. D. SOC 1 is designed for auditing controls over financial reporting

3. A. Information Security Policies, Supplier Relationships, and Compliance are all major elements of ISO 27001.

4. B. Transparency is a requirement of ISO 27018

5. A. Self-assessment is the least assurance in the STAR registry.

6. D. The StarAudit Framework is designed for European cloud consumption management.

7. B. Know the provider’s rules of engagement before doing testing on their platform.

8. A. Selecting a risk management framework is a good start to developing a robust risk and compliance program

9. C. The organization should choose to select “retention” since the likelihood and impact of the threats are low.

10. The SLE calculation contains the results of the exposure factor multiplied by the asset value