

# CISSP Exam Questions & CISSP Pdf Training & CISSP Latest Vce

 INFOSECTRAIN

## CISSP Practice Exam Questions and Answers

### Part-2

#### Domain 5 Identity and Access Management (IAM) (13%)

**Q.1. A company has discovered that an employee has been using a colleague's credentials to access sensitive information. What immediate action should the company take to address this issue?**

- A Ignore the issue as it is an internal matter
- B Terminate both employees involved
- C Conduct an investigation and enforce strict access control policies
- D Disable all user accounts temporarily

**Answer: C.** Conduct an investigation and enforce strict access control policies

**Explanation:** The first step is to conduct a comprehensive investigation to identify the scope of the issue and assess any potential impacts or unauthorized access.

**Q.2. What is the purpose of a Single Sign-On (SSO) system?**

- A To provide multi-factor authentication
- B To allow users to authenticate once and gain access to multiple systems
- C To monitor user activity on the network
- D To encrypt user passwords

[www.infosectrain.com](http://www.infosectrain.com)

03

BTW, DOWNLOAD part of ExamPrepAway CISSP dumps from Cloud Storage: <https://drive.google.com/open?id=1VEYYeZOMBvYISs60v8WQ7lAWX4sOzS3o>

ExamPrepAway ISC CISSP practice exam is the most thorough, most accurate and latest practice test. You will find that it is the only materials which can make you have confidence to overcome difficulties in the first. ISC CISSP exam certification are recognized in any country in the world and all countries will be treated equally. ISC CISSP Certification not only helps to improve your knowledge and skills, but also helps your career have more possibility.

ISC CISSP Certification is recognized globally as a benchmark for excellence in information security. It is highly valued by employers, and individuals who possess this certification are in high demand. Certified Information Systems Security Professional (CISSP) certification not only validates the skills and expertise of professionals in the field of information security, but it also demonstrates their commitment to the field and their dedication to ongoing professional development.

>> CISSP PDF Guide <<

## Reliable ISC CISSP Test Notes, CISSP Free Sample

Furthermore, there are up to 12 months of free real ISC CISSP exam questions updates available at ExamPrepAway. In conclusion, if your goal is to pass the ISC CISSP exam on your first attempt, the ExamPrepAway platform is the ideal choice. With its

comprehensive support and a money-back guarantee, as well as its expertly developed ISC CISSP Practice Exam, you can feel confident and prepare successfully for the ISC CISSP test.

## Elaborate the Format of the ISC CISSP Exam

The format of the ISC CISSP exam is:

- Free Response: The free-response section consists of one multiple-choice and three open-ended (short answer and essay questions). Performance Exam: This section includes performance tasks consisting of both open-ended and multiple-choice questions.
- Audio Questions: Audio questions are presented in this section. The candidate will listen to English language questions and read the related information from a provided reference document.

## ISC Certified Information Systems Security Professional (CISSP) Sample Questions (Q1258-Q1263):

### NEW QUESTION # 1258

What is the BEST way to encrypt web application communications?

- A. Transport Layer Security (TLS)
- B. Cipher Block Chaining Message Authentication Code (CBC-MAC)
- C. Secure Sockets Layer (SSL)
- D. Secure Hash Algorithm 1 (SHA-1)

**Answer: A**

Explanation:

Section: Software Development Security

### NEW QUESTION # 1259

According to best practice, which of the following is required when implementing third party software in a production environment?

- A. Scan the application for vulnerabilities
- B. Contract the vendor for patching
- C. Negotiate end user application training
- D. Escrow a copy of the software

**Answer: A**

Explanation:

According to best practice, one of the requirements when implementing third party software in a production environment is to scan the application for vulnerabilities. Vulnerabilities are weaknesses or flaws in the software that can be exploited by attackers to compromise the security, functionality, or performance of the system or network. Scanning the application for vulnerabilities can help to identify and mitigate the potential risks, ensure the compliance with the security policies and standards, and prevent the introduction of malicious code or backdoors. Contracting the vendor for patching, negotiating end user application training, and escrowing a copy of the software are all possible requirements when implementing third party software in a production environment, but they are not the most essential or best practice requirement of doing so. References: CISSP All-in-One Exam Guide, Eighth Edition, Chapter 8, Software Development Security, page 1018. Official (ISC)2 CISSP CBK Reference, Fifth Edition, Chapter 8, Software Development Security, page 1040.

### NEW QUESTION # 1260

A chemical plant wants to upgrade the Industrial Control System (ICS) to transmit data using Ethernet instead of RS422. The project manager wants to simplify administration and maintenance by utilizing the office network infrastructure and staff to implement this upgrade.

Which of the following is the GREATEST impact on security for the network?

- A. The ICS is now accessible from the office network
- B. The network administrators have no knowledge of ICS

- C. The ICS does not support the office password policy
- D. RS422 is more reliable than Ethernet

**Answer: A**

Explanation:

The greatest impact on security for the network is that the ICS is now accessible from the office network. This means that the ICS is exposed to more potential threats and vulnerabilities from the internet and the office network, such as malware, unauthorized access, data leakage, or denial-of-service attacks. The ICS may also have different security requirements and standards than the office network, such as availability, reliability, and safety. Therefore, connecting the ICS to the office network increases the risk of compromising the confidentiality, integrity, and availability of the ICS and the critical infrastructure it controls.

### NEW QUESTION # 1261

In a PKI infrastructure where are list of revoked certificates stored?

- A. Recovery Agent
- B. Registration Authority
- **C. CRL**
- D. Key escrow

**Answer: C**

Explanation:

Certificate revocation is the process of revoking a certificate before it expires.

A certificate may need to be revoked because it was stolen, an employee moved to a new company, or someone has had their access revoked. A certificate revocation is handled either through a Certificate Revocation List (CRL) or by using the Online Certificate Status Protocol (OCSP).

A repository is simply a database or database server where the certificates are stored. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known/compromised.

The owner of a certificate can request it be revoked at any time, or the request can be made by the administrator. The CA marks the certificate as revoked. This information is published in the CRL. The revocation process is usually very quick; time is based on the publication interval for the CRL.

Disseminating the revocation information to users may take longer. Once the certificate has been revoked, it can never be used-or trusted-again. The CA publishes the CRL on a regular basis, usually either hourly or daily. The CA sends or publishes this list to organizations that have chosen to receive it; the publishing process occurs automatically in the case of PKI. The time between when the CRL is issued and when it reaches users may be too long for some applications. This time gap is referred to as latency.

OCSP solves the latency problem: If the recipient or relaying party uses OCSP for verification, the answer is available immediately.

The following answers are incorrect:

**Registration Authority (RA)** A registration authority (RA) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it. RAs are part of a public key infrastructure (PKI), a networked system that enables companies and users to exchange information and money safely and securely. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.

**Recovery agent** Sometimes it is necessary to recover a lost key. One of the problems that often arises regarding PKI is the fear that documents will become lost forever-irrecoverable because someone loses or forgets his private key. Let's say that employees use Smart Cards to hold their private keys. If a user was to leave his Smart Card in his or her wallet that was left in the pants that he or she accidentally threw into the washing machine, then that user might be without his private key and therefore incapable of accessing any documents or e-mails that used his existing private key.

Many corporate environments implement a key recovery server solely for the purpose of backing up and recovering keys. Within an organization, there typically is at least one key recovery agent. A key recovery agent has the authority and capability to restore a user's lost private key. Some key recovery servers require that two key recovery agents retrieve private user keys together for added security. This is similar to certain bank accounts, which require two signatures on a check for added security. Some key recovery servers also have the ability to function as a key escrow server, thereby adding the ability to split the keys onto two separate recovery servers, further increasing security.

**Key escrow** (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the

contents of encrypted communications.

The following reference(s) were/was used to create this question: Dulaney, Emmett (2011-06-03). CompTIA Security+ Study Guide: Exam SY0-301 (pp. 347-348). John Wiley and Sons. Kindle Edition. and [http://en.wikipedia.org/wiki/Key\\_escrow](http://en.wikipedia.org/wiki/Key_escrow) and <http://my.safaribooksonline.com/book/certification/securityplus/9781597494267/public-keyinfrastructure/ch12lev1sec5> and <http://searchsecurity.techtarget.com/definition/registration-authority>

### NEW QUESTION # 1262

Which of the following should exist in order to perform a security audit?

- A. Neutrality of the auditor
- B. Industry framework to audit against
- C. Internal certified auditor
- D. External (third-party) auditor

**Answer: A**

### NEW QUESTION # 1263

.....

**Reliable CISSP Test Notes:** <https://www.examprepaway.com/ISC/braindumps.CISSP.ete.file.html>

- Ample Study Material for ISC CISSP Exam Questions - Attain Exam Success \* Search for ☀ CISSP ☀ on ( [www.prepawayexam.com](http://www.prepawayexam.com) ) immediately to obtain a free download ☐ CISSP Latest Questions
- CISSP Valid Test Cost ☐ Test CISSP Engine Version ☐ Test CISSP Engine Version ☐ Download ☐ CISSP ☐ for free by simply entering ☀ [www.pdfvce.com](http://www.pdfvce.com) ☐ website ☐ CISSP New Real Exam
- Pass Guaranteed Quiz 2026 ISC CISSP – Reliable PDF Guide ☐ Search for ➡ CISSP ☐ and download it for free on ⇒ [www.examcollectionpass.com](http://www.examcollectionpass.com) ⇐ website ☐ Exam CISSP Passing Score
- CISSP Exam PDF ☐ Download CISSP Free Dumps ☐ CISSP Valid Test Tips ☐ Download ☀ CISSP ☀ for free by simply entering “ [www.pdfvce.com](http://www.pdfvce.com) ” website ☐ CISSP New Real Exam
- Valid ISC CISSP Questions - Latest Release To Pass ISC Exam ☐ Enter [ [www.practicevce.com](http://www.practicevce.com) ] and search for ☀ CISSP ☀ to download for free ☐ CISSP New Dumps Ppt
- Valid ISC CISSP Questions - Latest Release To Pass ISC Exam ♥ ☐ Download ➤ CISSP ☐ for free by simply entering ☐ [www.pdfvce.com](http://www.pdfvce.com) ☐ website ☐ Exam CISSP Collection Pdf
- CISSP New Real Exam ☐ Latest CISSP Material ☐ Valid CISSP Test Cram ☐ Search for ✓ CISSP ☐ ✓ ☐ and obtain a free download on ➡ [www.vce4dumps.com](http://www.vce4dumps.com) ☐ ☐ CISSP Latest Test Cost
- 2026 CISSP PDF Guide: Certified Information Systems Security Professional (CISSP) - High Pass-Rate ISC Reliable CISSP Test Notes ☐ Search for ▶ CISSP ◀ and easily obtain a free download on [ [www.pdfvce.com](http://www.pdfvce.com) ] ☐ New CISSP Real Test
- Valid ISC CISSP Questions - Latest Release To Pass ISC Exam ☐ Open 【 [www.pdfdumps.com](http://www.pdfdumps.com) 】 enter { CISSP } and obtain a free download ☐ CISSP Labs
- Pass Guaranteed Quiz 2026 ISC CISSP – Reliable PDF Guide 🖱 Open website [ [www.pdfvce.com](http://www.pdfvce.com) ] and search for 「 CISSP 」 for free download ☐ CISSP New Real Exam
- CISSP Labs ☐ CISSP Online Bootcamps ☐ CISSP New Real Exam ☐ Immediately open 「 [www.prepawayexam.com](http://www.prepawayexam.com) 」 and search for ▶ CISSP ◀ to obtain a free download ☐ Exam CISSP Sample
- [www.zazzle.com](http://www.zazzle.com), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [myportal.utt.edu.tt](http://myportal.utt.edu.tt), [www.stes.tyc.edu.tw](http://www.stes.tyc.edu.tw), [hhi.instructure.com](http://hhi.instructure.com), [bbs.linyiapp.com](http://bbs.linyiapp.com), [yca.instructure.com](http://yca.instructure.com), [backloggd.com](http://backloggd.com), Disposable vapes

P.S. Free & New CISSP dumps are available on Google Drive shared by ExamPrepAway: <https://drive.google.com/open?id=1VEYYeZOmbylSs60v8WQ71AWX4sOzS3o>