

Exam Questions CISSP-ISSAP

Information Systems Security Architecture Professional

<https://www.2passeasy.com/dumps/CISSP-ISSAP/>



NEW QUESTION 1

Which of the following elements of planning gap measures the gap between the total potential for the market and the actual current usage by all the consumers in the market?

- A. Project gap
- B. Product gap
- C. Competitive gap
- D. Usage gap

Answer: D

NEW QUESTION 2

Peter works as a Network Administrator for Net World Inc. The company wants to allow remote users to connect and access its private network through a dial-up connection via the Internet. All the data will be sent across a public network. For security reasons, the management wants the data sent through the Internet to be encrypted. The company plans to use a Layer 2 Tunneling Protocol (L2TP) connection. Which communication protocol will Peter use to accomplish the task?

- A. IP Security (IPSec)
- B. Microsoft Point-to-Point Encryption (MPPE)
- C. Pretty Good Privacy (PGP)
- D. Data Encryption Standard (DES)

Answer: A

NEW QUESTION 3

Which of the following protocols multicasts messages and information among all member devices in an IP multicast group?

- A. ARP
- B. ICMP
- C. TCP
- D. IGMP

Answer: D

NEW QUESTION 4

Which of the following statements about a stream cipher are true? Each correct answer represents a complete solution. Choose three.

- A. It typically executes at a higher speed than a block ciphe
- B. It divides a message into blocks for processin
- C. It typically executes at a slower speed than a block ciphe
- D. It divides a message into bits for processin
- E. It is a symmetric key ciphe

Answer: ADE

NEW QUESTION 5

You are the Security Consultant advising a company on security methods. This is a highly secure location that deals with sensitive national defense related data. They are very concerned about physical security as they had a breach last month. In that breach an individual had simply grabbed a laptop and ran out of the building. Which one of the following would have been most effective in preventing this?

- A. Not using laptop
- B. Keeping all doors locked with a guar
- C. Using a man-tra
- D. A sign in lo

Answer: C

NEW QUESTION 6

Maria works as a Network Security Officer for Gentech Inc. She wants to encrypt her network traffic. The specific requirement for the encryption algorithm is that it must be a symmetric key block cipher. Which of the following techniques will she use to fulfill this requirement?

- A. IDEA
- B. PGP
- C. DES
- D. AES

Answer: C

NEW QUESTION 7

Which of the following attacks can be overcome by applying cryptography?

- A. Web ripping
- B. DoS
- C. Sniffing
- D. Buffer overflow

Answer: C

NEW QUESTION 8

Which of the following authentication methods prevents unauthorized execution of code on remote systems?

- A. TACACS
- B. S-RPC
- C. RADIUS
- D. CHAP

Answer: B

NEW QUESTION 9

Andrew works as a Network Administrator for Infonet Inc. The company's network has a Web server that hosts the company's Web site. Andrew wants to increase the security of the Web site by implementing Secure Sockets Layer (SSL). Which of the following types of encryption does SSL use? Each correct answer represents a complete solution. Choose two.

- A. Synchronous
- B. Secret
- C. Asymmetric
- D. Symmetric

Answer: CD

NEW QUESTION 10

You have decided to implement video surveillance in your company in order to enhance network security. Which of the following locations must have a camera in order to provide the minimum level of security for the network resources? Each correct answer represents a complete solution. Choose two.

- A. Parking lot
- B. All hallways
- C. Server Rooms
- D. All offices
- E. All entrance doors

Answer: CE

NEW QUESTION 10

You work as a Network Administrator for NetTech Inc. You want to have secure communication on the company's intranet. You decide to use public key and private key pairs. What will you implement to accomplish this?

- A. Microsoft Internet Information Server (IIS)
- B. VPN
- C. FTP server
- D. Certificate server

Answer: D

NEW QUESTION 12

Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead-space?

- A. Man trap
- B. Biometric device
- C. Host Intrusion Detection System (HIDS)
- D. Network Intrusion Detection System (NIDS)

Answer: A

NEW QUESTION 14

Which of the following are the initial steps required to perform a risk analysis process? Each correct answer represents a part of the solution. Choose three.

- A. Estimate the potential losses to assets by determining their value
- B. Establish the threats likelihood and regularity
- C. Valuations of the critical assets in hard cost
- D. Evaluate potential threats to the asset

Answer: ABD

NEW QUESTION 15

Which of the following are the primary components of a discretionary access control (DAC) model? Each correct answer represents a complete solution. Choose two.

- A. User's group
- B. File and data ownership
- C. Smart card

D. Access rights and permissions

Answer: BD

NEW QUESTION 18

You are the Network Administrator for a college. You watch a large number of people (some not even students) going in and out of areas with campus computers (libraries, computer labs, etc.). You have had a problem with laptops being stolen. What is the most cost effective method to prevent this?

- A. Smart card access to all areas with computer
- B. Use laptop lock
- C. Video surveillance on all areas with computer
- D. Appoint a security guar

Answer: B

NEW QUESTION 20

The ATM of a bank is robbed by breaking the ATM machine. Which of the following physical security devices can now be used for verification and historical analysis of the ATM robbery?

- A. Key card
- B. Biometric devices
- C. Intrusion detection systems
- D. CCTV Cameras

Answer: D

NEW QUESTION 21

Which of the following protocols is designed to efficiently handle high-speed data over wide area networks (WANs)?

- A. PPP
- B. X.25
- C. Frame relay
- D. SLIP

Answer: C

NEW QUESTION 26

Which of the following statements best describes a certification authority?

- A. A certification authority is a technique to authenticate digital documents by using computer cryptograph
- B. A certification authority is a type of encryption that uses a public key and a private key pair for data encryptio
- C. A certification authority is an entity that issues digital certificates for use by other partie
- D. A certification authority is a type of encryption that uses a single key to encrypt and decrypt dat

Answer: C

NEW QUESTION 29

Which of the following should the administrator ensure during the test of a disaster recovery plan?

- A. Ensure that the plan works properly
- B. Ensure that all the servers in the organization are shut dow
- C. Ensure that each member of the disaster recovery team is aware of their responsibilit
- D. Ensure that all client computers in the organization are shut dow

Answer: AC

NEW QUESTION 33

Kerberos is a computer network authentication protocol that allows individuals communicating over a non-secure network to prove their identity to one another in a secure manner. Which of the following statements are true about the Kerberos authentication scheme? Each correct answer represents a complete solution. Choose all that apply.

- A. Kerberos requires continuous availability of a central serve
- B. Dictionary and brute force attacks on the initial TGS response to a client may reveal the subject's password
- C. Kerberos builds on Asymmetric key cryptography and requires a trusted third part
- D. Kerberos requires the clocks of the involved hosts to be synchronize

Answer: ABD

NEW QUESTION 36

A helpdesk technician received a phone call from an administrator at a remote branch office. The administrator claimed to have forgotten the password for the root account on UNIX servers and asked for it. Although the technician didn't know any administrator at the branch office, the guy sounded really friendly and since he knew the root password himself, he supplied the caller with the password. What type of attack has just occurred?

- A. Social Engineering attack
- B. Brute Force attack

- C. War dialing attack
- D. Replay attack

Answer: A

NEW QUESTION 41

The IPSec protocol is configured in an organization's network in order to maintain a complete infrastructure for secured network communications. IPSec uses four components for this. Which of the following components reduces the size of data transmitted over congested network connections and increases the speed of such networks without losing data?

- A. AH
- B. ESP
- C. IPcomp
- D. IKE

Answer: C

NEW QUESTION 46

You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You want to perform the following tasks: Develop a risk-driven enterprise information security architecture. Deliver security infrastructure solutions that support critical business initiatives. Which of the following methods will you use to accomplish these tasks?

- A. Service-oriented architecture
- B. Sherwood Applied Business Security Architecture
- C. Service-oriented modeling framework
- D. Service-oriented modeling and architecture

Answer: B

NEW QUESTION 47

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

- A. Discretionary Access Control (DAC)
- B. Role Based Access Control (RBAC)
- C. Mandatory Access Control (MAC)
- D. Access Control List (ACL)

Answer: C

NEW QUESTION 49

You work as a Network Administrator for Blue Bell Inc. The company has a TCP-based network. The company has two offices in different cities. The company wants to connect the two offices by using a public network. You decide to configure a virtual private network (VPN) between the offices. Which of the following protocols is used by VPN for tunneling?

- A. L2TP
- B. HTTPS
- C. SSL
- D. IPSec

Answer: A

NEW QUESTION 50

Adam works as a Network Administrator. He discovers that the wireless AP transmits 128 bytes of plaintext, and the station responds by encrypting the plaintext. It then transmits the resulting ciphertext using the same key and cipher that are used by WEP to encrypt subsequent network traffic. Which of the following types of authentication mechanism is used here?

- A. Pre-shared key authentication
- B. Open system authentication
- C. Shared key authentication
- D. Single key authentication

Answer: C

NEW QUESTION 51

The OSI model is the most common networking model used in the industry. Applications, network functions, and protocols are typically referenced using one or more of the seven OSI layers. Of the following, choose the two best statements that describe the OSI layer functions. Each correct answer represents a complete solution. Choose two.

- A. Layers 1 and 2 deal with application functionality and data formatting
- B. These layers reside at the top of the model
- C. Layers 4 through 7 define the functionality of IP Addressing, Physical Standards, and Data Link protocol
- D. Layers 5, 6, and 7 focus on the Network Application, which includes data formatting and session control
- E. Layers 1, 2, 3, and 4 deal with physical connectivity, encapsulation, IP Addressing, and Error Recovery
- F. These layers define the end-to-end functions of data delivery

Answer: CD

NEW QUESTION 53

John works as a security manager for SoftTech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

- A. Evacuation drill
- B. Walk-through drill
- C. Structured walk-through test
- D. Full-scale exercise

Answer: C

NEW QUESTION 56

In software development, which of the following analysis is used to document the services and functions that have been accidentally left out, deliberately eliminated or still need to be developed?

- A. Gap analysis
- B. Requirement analysis
- C. Cost-benefit analysis
- D. Vulnerability analysis

Answer: A

NEW QUESTION 61

Which of the following schemes is used by the Kerberos authentication?

- A. Public key cryptography
- B. One time password
- C. Private key cryptography
- D. OPIE

Answer: C

NEW QUESTION 64

Which of the following are the centralized administration technologies? Each correct answer represents a complete solution. Choose all that apply.

- A. RADIUS
- B. TACACS+
- C. Media Access control
- D. Peer-to-Peer

Answer: AB

NEW QUESTION 69

Which of the following are used to suppress paper or wood fires? Each correct answer represents a complete solution. Choose two.

- A. Soda acid
- B. Kerosene
- C. Water
- D. CO2

Answer: AC

NEW QUESTION 71

Fill in the blank with the appropriate security method. _____ is a system, which enables an authority to control access to areas and resources in a given physical facility, or computer- based information system.

- A. Access control

Answer: A

NEW QUESTION 72

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Annualized Rate of Occurrence (ARO)
- C. Single Loss Expectancy (SLE)
- D. Exposure Factor (EF)

Answer: B

NEW QUESTION 73

You work as a Chief Security Officer for Tech Perfect Inc. The company has a TCP/IP based network. You want to use a firewall that can track the state of active connections of the network and then determine which network packets are allowed to enter through the firewall. Which of the following firewalls has this feature?

- A. Stateful packet inspection firewall
- B. Proxy-based firewall
- C. Dynamic packet-filtering firewall
- D. Application gateway firewall

Answer: C

NEW QUESTION 77

Fill in the blank with the appropriate security device. _____ is a device that contains a physical mechanism or electronic sensor that quantifies motion that can be either integrated with or connected to other devices that alert the user of the presence of a moving object within the field of view.

- A. Motion detector

Answer: A

NEW QUESTION 81

Which of the following methods will allow data to be sent on the Internet in a secure format?

- A. Serial Line Interface Protocol
- B. Point-to-Point Protocol
- C. Browsing
- D. Virtual Private Networks

Answer: D

NEW QUESTION 83

Which of the following are natural environmental threats that an organization faces? Each correct answer represents a complete solution. Choose two.

- A. Strikes
- B. Floods
- C. Accidents
- D. Storms

Answer: BD

NEW QUESTION 88

A company named Money Builders Inc., hires you to provide consultancy for setting up their Windows network. The company's server room will be in a highly secured environment. You are required to suggest an authentication method for it. The CFO of the company wants the server to use thumb impressions for authentication. Which of the following authentication methods will you suggest?

- A. Certificate
- B. Smart card
- C. Two-factor
- D. Biometrics

Answer: D

NEW QUESTION 89

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Integrity
- B. Availability
- C. Authenticity
- D. Confidentiality

Answer: D

NEW QUESTION 94

Which of the following backup types backs up files that have been added and all data that have been modified since the most recent backup was performed?

- A. Differential backup
- B. Incremental backup
- C. Daily backup
- D. Full backup

Answer: B

NEW QUESTION 99

Which of the following are the goals of a public key infrastructure (PKI)? Each correct answer represents a part of the solution. Choose all that apply.

- A. Authenticity
- B. Globalization
- C. Mobility

- D. Integrity
- E. Confidentiality
- F. Nonrepudiation

Answer: ADEF

NEW QUESTION 102

Which of the following encryption modes has the property to allow many error correcting codes to function normally even when applied before encryption?

- A. OFB mode
- B. CFB mode
- C. CBC mode
- D. PCBC mode

Answer: A

NEW QUESTION 105

Which of the following protocols provides the highest level of VPN security with a VPN connection that uses the L2TP protocol?

- A. IPSec
- B. PPPoE
- C. PPP
- D. TFTP

Answer: A

NEW QUESTION 110

You are the Network Administrator for a bank. In addition to the usual security issues, you are concerned that your customers could be the victim of phishing attacks that use fake bank Web sites. Which of the following would protect against this?

- A. MAC
- B. Mutual authentication
- C. Three factor authentication
- D. Two factor authentication

Answer: B

NEW QUESTION 114

Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

- A. $SLE = \text{Asset Value (AV)} * \text{Exposure Factor (EF)}$
- B. $SLE = \text{Asset Value (AV)} * \text{Annualized Rate of Occurrence (ARO)}$
- C. $SLE = \text{Annualized Loss Expectancy (ALE)} * \text{Annualized Rate of Occurrence (ARO)}$
- D. $SLE = \text{Annualized Loss Expectancy (ALE)} * \text{Exposure Factor (EF)}$

Answer: A

NEW QUESTION 115

Which of the following are man-made threats that an organization faces? Each correct answer represents a complete solution. Choose three.

- A. Theft
- B. Employee errors
- C. Strikes
- D. Frauds

Answer: ABD

NEW QUESTION 120

In which of the following access control models, owner of an object decides who is allowed to access the object and what privileges they have?

- A. Access Control List (ACL)
- B. Mandatory Access Control (MAC)
- C. Role Based Access Control (RBAC)
- D. Discretionary Access Control (DAC)

Answer: D

NEW QUESTION 125

Which of the following statements about Network Address Translation (NAT) are true? Each correct answer represents a complete solution. Choose three.

- A. It hides the internal IP addressing scheme
- B. It protects network from the password guessing attack
- C. It is used to connect private networks to the public Internet
- D. It shares public Internet addresses with a large number of internal network client

Answer: ACD

NEW QUESTION 130

Access control systems enable an authority to control access to areas and resources in a given physical facility or computer-based information system. Which of the following services provided by access control systems is used to determine what a subject can do?

- A. Authentication
- B. Authorization
- C. Accountability
- D. Identification

Answer: B

NEW QUESTION 133

Which of the following protocols should a Chief Security Officer configure in the network of his company to protect sessionless datagram protocols?

- A. SWIPE
- B. S/MIME
- C. SKIP
- D. SLIP

Answer: C

NEW QUESTION 135

Which of the following user authentications are supported by the SSH-1 protocol but not by the SSH-2 protocol? Each correct answer represents a complete solution. Choose all that apply.

- A. TIS authentication
- B. Rhosts (rsh-style) authentication
- C. Kerberos authentication
- D. Password-based authentication

Answer: ABC

NEW QUESTION 139

Fill in the blank with the appropriate encryption system. The _____ encryption system is an asymmetric key encryption algorithm for the public-key cryptography, which is based on the Diffie- Hellman key agreement.

- A. ElGamal

Answer: A

NEW QUESTION 144

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

- A. Install a network-based IDS
- B. Install a host-based IDS
- C. Install a DMZ firewall
- D. Enable verbose logging on the firewall

Answer: A

NEW QUESTION 149

You work as a Chief Security Officer for Tech Perfect Inc. The company has an internal room without any window and is totally in darkness. For security reasons, you want to place a device in the room. Which of the following devices is best for that room?

- A. Photoelectric motion detector
- B. Badge
- C. Closed-circuit television
- D. Alarm

Answer: A

NEW QUESTION 150

Which of the following are used to suppress gasoline and oil fires? Each correct answer represents a complete solution. Choose three.

- A. Water
- B. CO2
- C. Halon
- D. Soda acid

Answer: BCD

NEW QUESTION 153

Fill in the blank with the appropriate phrase. The is a simple document that provides a high-level view of the entire organization's disaster recovery efforts.

A. Executive summary

Answer: A

NEW QUESTION 154

You work as a Chief Security Officer for Tech Perfect Inc. You have configured IPSec and ISAKMP protocol in the company's network in order to establish a secure communication infrastructure. ccording to the Internet RFC 2408, which of the following services does the ISAKMP protocol offer to the network? Each correct answer represents a part of the solution. Choose all that apply.

- A. It relies upon a system of security association
- B. It provides key generation mechanism
- C. It authenticates communicating peer
- D. It protects against threats, such as DoS attack, replay attack, et

Answer: BCD

NEW QUESTION 159

Which of the following ports must be opened on the firewall for the VPN connection using Point-to- Point Tunneling Protocol (PPTP)?

- A. TCP port 110
- B. TCP port 443
- C. TCP port 5060
- D. TCP port 1723

Answer: D

NEW QUESTION 160

Which of the following plans is a comprehensive statement of consistent actions to be taken before, during, and after a disruptive event that causes a significant loss of information systems resources?

- A. Disaster recovery plan
- B. Contingency plan
- C. Business Continuity plan
- D. Continuity of Operations plan

Answer: A

NEW QUESTION 163

Which of the following types of ciphers operates on a group of bits rather than an individual character or bit of a message?

- A. Block cipher
- B. Classical cipher
- C. Substitution cipher
- D. Stream cipher

Answer: A

NEW QUESTION 168

Which of the following techniques can be used by an administrator while working with the symmetric encryption cryptography? Each correct answer represents a complete solution. Choose all that apply.

- A. Block cipher
- B. Stream cipher
- C. Transposition cipher
- D. Message Authentication Code

Answer: ABD

NEW QUESTION 170

Which of the following is a form of gate that allows one person to pass at a time?

- A. Biometric
- B. Man-trap
- C. Turnstile
- D. Fence

Answer: C

NEW QUESTION 173

Which of the following algorithms can be used to check the integrity of a file?

- A. md5

- B. rsa
- C. blowfish
- D. sha

Answer: AD

NEW QUESTION 174

The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

- A. Service-oriented business integration modeling
- B. Service-oriented logical design modeling
- C. Service-oriented discovery and analysis modeling
- D. Service-oriented logical architecture modeling

Answer: D

NEW QUESTION 178

Which of the following security architectures defines how to integrate widely disparate applications for a world that is Web-based and uses multiple implementation platforms?

- A. Sherwood Applied Business Security Architecture
- B. Service-oriented modeling and architecture
- C. Enterprise architecture
- D. Service-oriented architecture

Answer: D

NEW QUESTION 179

The OSI reference model is divided into layers and each layer has a specific task to perform. At which layer of OSI model is the File and Print service performed?

- A. Session layer
- B. Presentation layer
- C. Transport layer
- D. Application layer

Answer: D

NEW QUESTION 180

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering? Each correct answer represents a complete solution. Choose two.

- A. Reduce power consumption
- B. Ease of maintenance
- C. Failover
- D. Load balancing

Answer: AB

NEW QUESTION 182

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

- A. Risk acceptance
- B. Risk avoidance
- C. Risk transfer
- D. Risk mitigation

Answer: C

NEW QUESTION 183

You work as a Network Consultant. A company named Tech Perfect Inc. hires you for security reasons. The manager of the company tells you to establish connectivity between clients and servers of the network which prevents eavesdropping and tampering of data on the Internet. Which of the following will you configure on the network to perform the given task?

- A. WEP
- B. IPsec
- C. VPN
- D. SSL

Answer: D

NEW QUESTION 186

The security controls that are implemented to manage physical security are divided in various groups. Which of the following services are offered by the administrative physical security control group? Each correct answer represents a part of the solution. Choose all that apply.

- A. Construction and selection
- B. Site management
- C. Awareness training
- D. Access control
- E. Intrusion detection
- F. Personnel control

Answer: ABCF

NEW QUESTION 191

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual CISSP-ISSAP Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the CISSP-ISSAP Product From:

<https://www.2passeasy.com/dumps/CISSP-ISSAP/>

Money Back Guarantee

CISSP-ISSAP Practice Exam Features:

- * CISSP-ISSAP Questions and Answers Updated Frequently
- * CISSP-ISSAP Practice Questions Verified by Expert Senior Certified Staff
- * CISSP-ISSAP Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * CISSP-ISSAP Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year