CISSP Q&As

Certified Information Systems Security Professional

Pass ISC CISSP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/CISSP.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following violates identity and access management best practices?

A. User accounts

B. System accounts

C. Generic accounts

D. Privileged accounts

Correct Answer: C

QUESTION 2

Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.

B. Encrypted messages are only decrypted by the final node.

C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.

D. Only secure nodes are used in this type of transmission.

Correct Answer: C

Explanation: In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.

Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re-encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the

transmission path is compromised.

Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the

packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods.

Link encryption provides protection against packet sniffers and eavesdroppers.

In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846).

McGraw-Hill.

And:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 132).

QUESTION 3

An expert system that has rules of the form If w is low and x is high then y is intermediate, where w and x are input variables and y is the output variable, is called a:

A. Fuzzy expert system

B. Realistic expert system

C. Neural network

D. Boolean expert system

Correct Answer: A

A fuzzy expert system is an expert system that uses fuzzy membership functions and rules, instead of Boolean logic, to reason about data. Thus, fuzzy variables can have an approximate range of values instead of the binary True or False

used in conventional expert systems. When it is desired to convert the fuzzy output to a single value, defuzzification is used. One approach to defuzzification is the CENTROID method. With this method, a value of the output variable is

computed by finding the variable value of the center of gravity of the membership function for the fuzzy output value.

Answers Neural network and Realistic expert system are distracters, and answer Boolean expert system is incorrect since it refers to Boolean values of one or zero.

QUESTION 4

Making sure that only those who are supposed to access the data can access is which of the following?

A. confidentiality.

B. capability.

C. integrity.

D. availability.

Correct Answer: A

Explanation: From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it. Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 59.

QUESTION 5

What should happen when an emergency change to a system must be performed?

A. The change must be given priority at the next meeting of the change control board.

B. Testing and approvals must be performed quickly.

C. The change must be performed immediately and then submitted to the change board.

D. The change is performed and a notation is made in the system log.

Correct Answer: B

QUESTION 6

Why do buffer overflows happen?

A. Because buffers can only hold so much data.

B. Because input data is not checked for appropriate length at time of input.

C. Because they are an easy weakness to exploit.

D. Because of insufficient system memory.

Correct Answer: B

QUESTION 7

In the OSI/ISO model, at what level is SET (SECURE ELECTRONIC TRANSACTION PROTOCOL) provided?

A. Application

B. Network

C. Presentation

D. Session

Correct Answer: A

Explanation: This protocol was created by VISA and MasterCard as a common effort to make the buying process over the Internet secure through the distribution line of those companies. It is located in layer 7 of the OSI model, the application layer. SET uses a system of locks and keys along with certified account IDs for both consumers and merchants. Then, through a unique process of "encrypting" or scrambling the information exchanged between the shopper and the online store, SET ensures a payment process that is convenient, private and most of all secure.

QUESTION 8

The structures, transmission methods, transport formats, and security measures that are used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media includes?

A. The Telecommunications and Network Security domain.

B. The Telecommunications and Netware Security domain.

C. The Technical communications and Network Security domain.

D. The Telnet and Network Security domain.

Correct Answer: A

Explanation: This is pretty straight forward. The four principal pillars of computer security:

integrity, authentication, confidentiality and availability are all part of the network security and telecommunication domain. Why? Because those pillars deal with that. We provide integrity through digital signatures, authentication through

passwords, confidentiality through encryption and availability by fault tolerance and disaster recovery. All of those are networking and telecommunication components.

QUESTION 9

Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop

B. Smurf

C. Ping of Death

D. SYN flood

E. SNMP Attack

Correct Answer: A

Explanation: The teardrop attack uses overlapping packet fragments to confuse a target system and cause the system to reboot or crash.

QUESTION 10

The Diffie-Hellman algorithm is used for:

A. Encryption

B. Digital signature

C. Key agreement

D. Non-repudiation

Correct Answer: C

Explanation: The Diffie-Hellman algorithm is used for Key agreement (key distribution) and cannot be used to encrypt and decrypt messages. Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page

4).

Note: key agreement, is different from key exchange, the functionality used by the other asymmetric algorithms.

AIO, third edition Cryptography (Page 632)

AIO, fourth edition Cryptography (Page 709)

QUESTION 11

Which of the following is NOT true of Secure Sockets Layer (SSL)?

A. By convention it uses \\'s-http://\\' instead of \\'http://\\'.

B. Is the predecessor to the Transport Layer Security (TLS) protocol.

C. It was developed by Netscape.

D. It is used for transmitting private information, data, and documents over the Internet.

Correct Answer: A

Explanation: Web pages that use SSL use \\'https://\\' instead of \\'http://\\', whereas documents that use Secure-http start with s-http://.

The following answers are incorrect:

Is the predecessor to Transport Layer Security, It was developed by Netscape, and It is used for transmitting private documents over the Internet.

As these are all TRUE answers, therefore incorrect for this question. References: TIPTON, Harold F. and HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, pages 496, 976

KRUTZ, Ronald L. and VINES, Russell Dean, The CISSP Prep Guide, Gold Edition, 2003, page 117

QUESTION 12

The standard process to certify and accredit

A. DIACAP

B. DITSCAP

C. CIAP

D. NIACAP

Correct Answer: B

The correct answer is DITSCAP, the Defense Information Technology Security Certification and Accreditation Process.

*

Answer NIACAP refers to the US government\\'s non-defense Certification and Accreditation (CandA) process the National Information Assurance Certification and Accreditation Process.

*

CIAP refers to the Commercial Information Security Analysis Process that is currently under development for application to commercial systems.

*

Answer DIACAP is a distracter.

QUESTION 13

Technical controls such as encryption and access control can be built into the operating system, be software applications, or can be supplemental hardware/software units. Such controls, also known as logical controls, represent which pairing?

A. Preventive/Administrative Pairing

B. Preventive/Technical Pairing

C. Preventive/Physical Pairing

D. Detective/Technical Pairing

Correct Answer: B

Explanation: Preventive/Technical controls are also known as logical controls and can be built into the operating system, be software applications, or can be supplemental hardware/software units. Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 34

QUESTION 14

Of the various types of "Hackers" that exist, the ones who are not worried about being caught and spending time in jail and have a total disregard for the law or police force, are labeled as what type of hackers?

A. Suicide Hackers

B. Black Hat Hackers

C. White Hat Hackers

D. Gray Hat Hackers

Correct Answer: A

Explanation: Suicide Hackers are a type of hackers without fear, who disregard the authority, the police, or law. Suicide Hackers hack for a cause important to them and find the end goal more important than their individual freedom.

The term "Hacker" originally meant a Unix computer enthusiast but has been villainized in the media as a "Criminal Hacker" for a mass audience. A hacker used to be known as a good person who would add functionality within software or

would make things work better. To most people today "Hacker" means criminal "Criminal Cracker", it is synonymous with Cracker or someone who get access to a system without the owner authorization.

As seen in news reports in 2011 and later hackers associated with the "Anonymous" movement have attacked finance and/or credit card companies, stolen enough information to make contributions to worthy charities on behalf of

organizations they see as contrary to the public good. These sorts of attackers/hackers could be considered suicide hackers. Some did get caught and prosecuted while carrying out their cause. Nobody can know if they knew their activities

would land them in court and/or prison but they had to have known of the risk and proceeded anyway.

The following answers are incorrect:

Black Hat hackers are also known as crackers and are merely hackers who "violates computer security for little reason beyond maliciousness or for personal gain". Black Hat Hackers are "the epitome of all that the public fears in a computer

criminal". Black Hat Hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

White Hat Hackers are law-abiding, reputable experts defending assets and not breaking laws. A white hat hacker breaks security for non-malicious reasons, for instance testing their own security system. The term "white hat" in Internet slang

refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. Often, this type of \\'white hat\\' hacker is called an ethical hacker. The

International Council of Electronic Commerce Consultants, also known as the EC-Council has developed certifications, courseware, classes, and online training covering the diverse arena of Ethical Hacking.

Note about White Hat: As reported by Adin Kerimov, a white hat would not be worried about going to jail as he is doing a test with authorization as well and he has a signed agreement. While this is a true point he BEST choice is Suicide

Hackers for the purpose of the exam, a white hat hacker would not disregard law and the autority. . Gray Hat Hackers work both offensively and defensively and can cross the border between legal/ethical behavior and illegal/unethical

behavior. A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been

hacked, for example. Then they may offer to repair their system for a small fee.

OTHER TYPES OF HACKERS

Elite hacker is a social status among hackers, elite is used to describe the most skilled. Newly discovered exploits will circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members.

Script kiddie A script kiddie(or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept--hence the term script (i.e.

a

prearranged plan or set of activities) kiddie (i.e. kid, child--an individual lacking knowledge and experience, immature). Often time they do not even understand how they are taken advantage of the system, they do not underrstand the

weakness being exploited, all they know is how to use a tool that somone else has built.

Neophyte A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking.

Hacktivist A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

The following reference(s) were/was used to create this question:

2011. EC-COUNCIL Official Curriculum, Ethical Hacking and Countermeasures, v7.1, Module 1, Page. 15.

and

https://en.wikipedia.org/wiki/Hacker_%28computer_security%29

QUESTION 15

Which one of the following considerations has the LEAST impact when considering transmission security?

A. Network availability

B. Data integrity

C. Network bandwidth

D. Node locations

Correct Answer: C

QUESTION 16

Which of the following risk handling technique involves the practice of passing on the risk to another entity, such as an insurance company?

A. Risk Mitigation

B. Risk Acceptance

C. Risk Avoidance

D. Risk transfer

Correct Answer: D

Explanation: Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

For your exam you should know below information about risk assessment and treatment:

A risk assessment, which is a tool for risk management, is a method of identifying vulnerabilities and threats and assessing the possible impacts to determine where to implement security controls. A risk assessment is carried out, and the

results are analyzed. Risk analysis is used to ensure that security is cost-effective, relevant, timely, and responsive to threats. Security can be quite complex, even for well-versed security professionals, and it is easy to apply too much

security, not enough security, or the wrong security controls, and to spend too much money in the process without attaining the necessary objectives. Risk analysis helps companies prioritize their risks and shows management the amount of

resources that should be applied to protecting against those risks in a sensible manner.

A risk analysis has four main goals:

?Identify assets and their value to the organization.

?Identify vulnerabilities and threats.

?Quantify the probability and business impact of these potential threats. ?Provide an economic balance between the impact of the threat and the cost of the countermeasure.

Treating Risk

Risk Mitigation

Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Examples of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. Risk Mitigation

involves applying appropriate control to reduce risk. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential organizations put countermeasures in place, such as firewalls, intrusion

detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information. In the underage driver example, risk mitigation could take the form of driver education for the youth or

establishing a policy not allowing the young driver to use a cell phone while driving, or not letting youth of a certain age have more than one friend in the car as a passenger at any given time.

Risk Transfer

Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way. The family is evaluating whether to permit an

underage driver to use the family car. The family decides that it is important for the youth to be mobile, so it transfers the financial risk of a youth being in an accident to the insurance company, which provides the family with auto insurance.

It is important to note that the transfer of risk may be accompanied by a cost. This is certainly true for the insurance example presented earlier, and can be seen in other insurance instances, such as liability insurance for a vendor or the

insurance taken out by companies to protect against hardware and software theft or destruction. This may also be true if an organization must purchase and implement security controls in order to make their organization less desirable to

attack. It is important to remember that not all risk can be transferred. While financial risk is simple to transfer through insurance, reputational risk may almost never be fully transferred.

Risk Avoidance

Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized. For example, have you ever heard a friend, or parents of a friend, complain about the costs of insuring an underage driver? How about the

risks that many of these children face as they become mobile? Some of these families will decide that the child in question will not be allowed to drive the family car, but will rather wait until he or she is of legal age (i.e., 18 years of age) before

committing to owning, insuring, and driving a motor vehicle.

In this case, the family has chosen to avoid the risks (and any associated benefits) associated with an underage driver, such as poor driving performance or the cost of insurance for the child. Although this choice may be available for some

situations, it is not available for all. Imagine a global retailer who, knowing the risks associated with doing business on the Internet, decides to avoid the practice. This decision will likely cost the company a significant amount of its revenue (if,

indeed, the company has products or services that consumers wish to purchase). In addition, the decision may require the company to build or lease a site in each of the locations, globally, for which it wishes to continue business. This could

have a catastrophic effect on the company\\'s ability to continue business operations

Risk Acceptance

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the

cost versus the benefit of dealing with the risk in another way.

For example, an executive may be confronted with risks identified during the course of a risk assessment for their organization. These risks have been prioritized by high, medium, and low impact to the organization. The executive notes that

in order to mitigate or transfer the low-level risks, significant costs could be involved. Mitigation might involve the hiring of additional highly skilled personnel and the purchase of new hardware, software, and office equipment, while

transference of the risk to an insurance company would require premium payments.

The executive then further notes that minimal impact to the organization would occur if any of the reported low-level threats were realized. Therefore, he or she (rightly) concludes that it is wiser for the organization to forgo the costs and

accept the risk. In the young driver example, risk acceptance could be based on the observation that the youngster has demonstrated the responsibility and maturity to warrant the parent\\'s trust in his or her judgment.

The following answers are incorrect:

Risk Transfer - Risk transfer is the practice of passing on the risk in question to another entity, such as an insurance company. Let us look at one of the examples that were presented above in a different way.

Risk avoidance - Risk avoidance is the practice of coming up with alternatives so that the risk in question is not realized.

Risk Mitigation - Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk

presented.

The following reference(s) were/was used to create this question:

CISA Review Manual 2014 Page number 51

and

Official ISC2 guide to CISSP CBK 3rd edition page number 534-536

QUESTION 17

Which choice below is an accurate statement about the difference between monitoring and auditing?

A. A system audit is an ongoing real-time activity that examines a system.

B. A system audit cannot be automated.

C. Monitoring is an ongoing activity that examines either the system or the users.

D. Monitoring is a one-time event to evaluate security.

Correct Answer: C

System audits and monitoring are the two methods organizations use to maintain operational assurance. Although the terms are used loosely within the computer security community, a system audit is a one-time or periodic event to evaluate security, whereas monitoring refers to an ongoing activity that examines either the system or the users. In general, the more real-time an activity is, the more it falls into the category of monitoring. Source: NIST Special Publication 800- 14, Generally Accepted Principles and Practices for Securing Information Technology Systems.

QUESTION 18

The SEI Software Capability Maturity Model is based on the premise that:

A. The quality of a software product is a direct function of the quality of its associated software development and maintenance processes.

B. The maturity of an organizations software processes cannot be measured.

C. Software development is an art that cannot be measured by conventional means.

D. Good software development is a function of the number of expert programmers in the organization.

Correct Answer: A

The quality of a software product is a direct

function of the quality of its associated software development and maintenance processes.

*Answer "Good software development is a function of the number of expert programmers in the organization" is false because the SEI Software CMM relates the production of good software to having the proper processes in place in an

organization and not to expert programs or heroes.

*Answer "The maturity of an organizations software processes cannot be measured" is false because the Software CMM provides means to measure the maturity of an organizations software processes.

*Answer " Software development is an art that cannot be measured by conventional means" is false because the Software CMM provides means to measure the maturity of an organizations software processes.

QUESTION 19

Which choice below is the correct definition of a Mutual Aid Agreement?

A. A management-level analysis that identifies the impact of losing an entitys resources

B. An appraisal or determination of the effects of a disaster on human, physical, economic, and natural resources

C. Activities taken to eliminate or reduce the degree of risk to life and property

D. A prearranged agreement to render assistance to the parties of the agreement

Correct Answer: D

Amutual aid agreement is used by two or more parties to provide for assistance if one of the parties experiences an emergency. It is expected that the other parties will assist the affected party in various ways, perhaps by making office space available, or computing time or resources, or supplying manpower if needed. While mutual aid agreements may be a very cost-effective solution for disaster recovery, it does not provide for full operations redundancy. An example of a problem with a total reliance on mutual aid would be the event that affects all parties to the agreement, thereby rendering the agreement useless. While they are an effective means to provide some resources to the organization in an emergency, they in themselves are not a replacement for a full disaster recovery plan, including alternate computer processing sites. *Answer "A management-level analysis that identifies the impact of losing an entitys resources" describes a business continuity plan.

*Answer "An appraisal or determination of the effects of a disaster on human, physical, economic, and natural resources" describes a damage assessment *answer "Activities taken to eliminate or reduce the degree of risk to life and property" describes risk mitigation.

Source: NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity, National Fire Protection Association, 2000 edition, and Emergency Management Guide for Business and Industry, Federal Emergency Management Agency, August 1998.

QUESTION 20

The Diffie-Hellman algorithm is used for?

A. Encryption

B. Digital signature

C. Key exchange

D. Non-repudiation

Correct Answer: C

Explanation: Diffie Hellman is a Key exchange algorithm, its strength its in the difficulty of computing discrete logarithms

in a finite field generated by a large primary number. Although RSA and Diffie Hellman are similar in mathematical theory, their implementation is somewhat different. This algorithm has been released to the public. It\\'s the primary alternative to the RSA algorithm for key exchange.

QUESTION 21

Which of the following are required components for implementing software configuration management systems?

A. Audit control and signoff

B. User training and acceptance

C. Rollback and recovery processes

D. Regression testing and evaluation

Correct Answer: C

QUESTION 22

Public key infrastructure(PKI) consists of programs, data formats, procedures, communication protocols, security policies, and public key cryptographic mechanisms working in a comprehensive manner to enable a wide range of dispersed people to communicate in a secure and predictable fashion.

This infrastructure is based upon which of the following Standard?

A. X.509

B. X.500

C. X.400

D. X.25

Correct Answer: A

Explanation: X.509 was initially issued on July 3, 1988 and was begun in association with the X.500 standard.

It assumes a strict hierarchical system of certificate authorities (CAs) for issuing the certificates. This contrasts with web of trust models, like PGP, where anyone (not just special CAs) may sign and thus attest to the validity of others\\' key

certificates.

PKI establishes a level of trust within an environment. PKI is an ISO authentication framework that uses public key cryptography and the X.509 standard.

The framework was set up to enable authentication to happen across different networks and the Internet.

Particular protocols and algorithms are not specified, which is why PKI is called a framework and not a specific technology.

In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate

revocation lists,

attribute certificates, and a certification path validation algorithm.

The standard for how the CA creates the certificate is X.509, which dictates the different fields used in the certificate and the valid values that can populate those fields.

The most commonly used version is v3 of this standard, which is often denoted as X.509v3.

Many cryptographic protocols use this type of certificate, including SSL.

The certificate includes the serial number, version number, identity information, algorithm information, lifetime dates, and the signature of the issuing authority

The following answers are incorrect:

X.500 is a Directory Access Protocol(LDAP)

X.400 is for Electronic Messaging (EMAILs)

X.25 is Frame Relay

The following reference(s) were/was used to create this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 833). McGraw- Hill . Kindle Edition.

QUESTION 23

Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.

B. The SSL protocol\\'s primary use is to authenticate the client to the server using public key cryptography and digital certificates.

C. Web pages using the SSL protocol start with HTTPS

D. SSL can be used with applications such as Telnet, FTP and email protocols.

Correct Answer: B

Explanation: All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the

server to the client.

The following reference(s) were used for this question:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 170).

QUESTION 24

What is the second phase of Public Key Infrastructure (PKI) key/certificate life-cycle management?

A. Implementation Phase

B. Initialization Phase

C. Cancellation Phase

D. Issued Phase

Correct Answer: D

QUESTION 25

For competitive reasons, the customers of a large shipping company called the "Integrated International Secure Shipping Containers Corporation" (IISSCC) like to keep private the various cargos that they ship. IISSCC uses a secure database system based on the Bell- LaPadula access control model to keep this information private. Different information in this database is classified at different levels. For example, the time and date a ship departs is labeled Unclassified, so customers can estimate when their cargos will arrive, but the contents of all shipping containers on the ship are labeled Top Secret to keep different shippers from viewing each other\\'s cargos.

An unscrupulous fruit shipper, the "Association of Private Fuit Exporters, Limited" (APFEL) wants to learn whether or not a competitor, the "Fruit Is Good Corporation" (FIGCO), is shipping pineapples on the ship "S.S. Cruise Pacific" (S.S. CP). APFEL can\\'t simply read the top secret contents in the IISSCC database because of the access model. A smart APFEL worker, however, attempts to insert a false, unclassified record in the database that says that FIGCO is shipping pineapples on the S.S. CP, reasoning that if there is already a FIGCO-pineapple-SSCP record then the insertion attempt will fail. But the attempt does not fail, so APFEL can\\'t be sure whether or not FIGCO is shipping pineapples on the S.S. CP.

What is the name of the access control model property that prevented APFEL from reading FIGCO\\'s cargo information? What is a secure database technique that could explain why, when the insertion attempt succeeded, APFEL was still unsure whether or not FIGCO was shipping pineapples?

A. *-Property and Polymorphism

B. Strong *-Property and Polyinstantiation

C. Simple Security Property and Polymorphism

D. Simple Security Property and Polyinstantiation

Correct Answer: D

Explanation: The Simple Security Property states that a subject at a given clearance may not read an object at a higher classification, so unclassified APFEL could not read FIGCO\\'s top secret cargo information.

Polyinstantiation permits a database to have two records that are identical except for their classifications (i.e., the primary key includes the classification). Thus, APFEL\\'s new unclassified record did not collide with the real, top secret record,

so APFEL was not able to learn about FIGs pineapples.

The following answers are incorrect:

*-Property and Polymorphism

The *-property states that a subject at a given clearance must not write to any object at a lower classification, which is irrelevant here because APFEL was trying to read data with a higher classification.

Polymorphism is a term that can refer to, among other things, viruses that can change their code to better hide from anti-virus programs or to objects of different types in an object- oriented program that are related by a common superclass

and can, therefore, respond to a common set of methods in different ways. That\\'s also irrelevant to this question.

Strong *-Property and Polyinstantiation

Half-right. The strong *-property limits a subject of a given clearance to writing only to objects with a matching classification. APFEL\\'s attempt to insert an unclassified record was consistent with this property, but that has nothing to do with

preventing APFEL from reading top secret information.

Simple Security Property and Polymorphism

Also half-right. See above for why Polymorphism is wrong.

The following reference(s) were/was used to create this question:

HARRIS, Shon, CISSP All-in-one Exam Guide, Third Edition, McGraw-Hill/Osborne, 2005

Chapter 5: Security Models and Architecture (page 280) Chapter 11: Application and System Development (page 828)

QUESTION 26

Why are maintenance accounts a threat to operations controls?

A. Maintenance might require physical access to the system by vendors or service providers.

B. Maintenance accounts are commonly used by hackers to access network devices.

C. Maintenance personnel could slip and fall and sue the organization.

D. Maintenance account information could be compromised if printed reports are left out in the open.

Correct Answer: B

Maintenance accounts are login accounts

to systems resources, primarily networked devices. They often have the factory-set passwords that are frequently distributed through the hacker community.

QUESTION 27

In which OSI layer does the MIDI digital music protocol standard reside?

A. Session Layer

B. Application Layer

C. Transport Layer

D. Presentation Layer

Correct Answer: D

The correct answer is Presentation Layer. MIDI is a Presentation layer protocol.

QUESTION 28

Which question below is NOT accurate regarding the process of risk assessment?

A. Risk assessment is the final result of the risk management methodology.

B. The likelihood of a threat must be determined as an element of the risk assessment.

C. Risk assessment is the first process in the risk management methodology

D. The level of impact of a threat must be determined as an element of the risk assessment.

Correct Answer: A

Risk is a function of the likelihood of a given threat-source\\'s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. Risk assessment is the first process in the risk management methodology. The risk assessment process helps organizations identify appropriate controls for reducing or eliminating risk during the risk mitigation process. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system. The likelihood that a potential vulnerability could be exercised by a given threatsource can be described as high, medium, or low. Impact refers to the magnitude of harm that could be caused by a threat\\'s exploitation of a vulnerability. The determination of the level of impact produces a relative value for the IT assets and resources affected. Source: NIST Special Publication 800-30, Risk Management Guide for Information Tech- nology Systems.

QUESTION 29

Examples of types of physical access controls include all except which of the following?

A. badges

B. locks

C. guards

D. passwords

Correct Answer: D

Explanation: A password is not a physical thing, it\\'s a logical one. You can control physical access with armed guards, by locking doors and using badges to open doors, but you can\\'t relate password to a physical environment. Just to remember, Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system. They are related to software, not to hardware.

QUESTION 30

Which encryption algorithm is BEST suited for communication with handheld wireless devices?

A. ECC (Elliptic Curve Cryptosystem)

B. RSA

C. SHA

D. RC4

Correct Answer: A

Explanation: As it provides much of the same functionality that RSA provides: digital signatures, secure key distribution,and encryption. One differing factor is ECC\\'s efficiency. ECC is more efficient that RSA and any other asymmetric

algorithm.

The following answers are incorrect because :

RSA is incorrect as it is less efficient than ECC to be used in handheld devices. SHA is also incorrect as it is a hashing algorithm. RC4 is also incorrect as it is a symmetric algorithm. Reference : Shon Harris AIO v3 , Chapter-8 : Cryptography

, Page : 631 , 638.

QUESTION 31

Which of the following DoD Model layer provides non-repudiation services?

A. network layer.

B. application layer.

C. transport layer.

D. data link layer.

Correct Answer: B

Explanation: The Application Layer determines the identity of the communication partners and this is where Non-Repudiation service would be provided as well. See the layers below:

DOD Model DoD Model

The following answers are incorrect:

network layer. Is incorrect because the Network Layer mostly has routing protocols, ICMP, IP, and IPSEC. It it not a layer in the DoD Model. It is called the Internet Layer within the DoD model.

transport layer. Is incorrect because the Transport layer provides transparent transfer of data between end users. This is called Host-to-Host on the DoD model but sometimes some books will call it Transport as well on the DoD model. data

link layer. Is incorrect because the Data Link Layer defines the protocols that computers must follow to access the network for transmitting and receiving messages. It is part of the OSI Model. This does not exist on the DoD model, it is called

the Link Layer on the DoD model.

QUESTION 32

A prolonged high voltage is a:

A. spike

B. blackout

C. surge

D. fault

Correct Answer: C

Explanation: A prolonged high voltage is a surge.

From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw- Hill/Osborne, 2005, page 368.

QUESTION 33

What can be defined as an abstract machine that mediates all access to objects by subjects to ensure that subjects have the necessary access rights and to protect objects from unauthorized access?

A. The Reference Monitor

B. The Security Kernel

C. The Trusted Computing Base

D. The Security Domain

Correct Answer: A

Explanation: The reference monitor refers to abstract machine that mediates all access to objects by subjects.

This question is asking for the concept that governs access by subjects to objects, thus the reference monitor is the best answer. While the security kernel is similar in nature, it is what actually enforces the concepts outlined in the reference

monitor.

In operating systems architecture a reference monitor concept defines a set of design requirements on a reference validation mechanism, which enforces an access control policy over subjects\\' (e.g., processes and users) ability to perform

operations (e.g., read and write) on objects (e.g., files and sockets) on a system. The properties of a reference monitor are:

The reference validation mechanism must always be invoked (complete mediation). Without this property, it is possible for an attacker to bypass the mechanism and violate the security policy.

The reference validation mechanism must be tamperproof (tamperproof). Without this property, an attacker can undermine the mechanism itself so that the security policy is not correctly enforced.

The reference validation mechanism must be small enough to be subject to analysis and tests, the completeness of which can be assured (verifiable). Without this property, the mechanism might be flawed in such a way that the policy is not

enforced.

For example, Windows 3.x and 9x operating systems were not built with a reference monitor, whereas the Windows NT line, which also includes Windows 2000 and Windows XP, was designed to contain a reference monitor, although it is not

clear that its properties (tamperproof, etc.) have ever been independently verified, or what level of computer security it was intended to provide.

The claim is that a reference validation mechanism that satisfies the reference monitor concept will correctly enforce a system\\'s access control policy, as it must be invoked to mediate all security-sensitive operations, must not be tampered,

and has undergone complete analysis and testing to verify correctness. The abstract model of a reference monitor has been widely applied to any type of system that needs to enforce access control, and is considered to express the

necessary and sufficient properties for any system making this security claim.

According to Ross Anderson, the reference monitor concept was introduced by James Anderson in an influential 1972 paper.

Systems evaluated at B3 and above by the Trusted Computer System Evaluation Criteria (TCSEC) must enforce the reference monitor concept. The reference monitor, as defined in AIO V5 (Harris) is: "an access control concept that refers to

an abstract machine that mediates all access to objects by subjects."

The security kernel, as defined in AIO V5 (Harris) is: "the hardware, firmware, and software elements of a trusted computing based (TCB) that implement the reference monitor concept. The kernel must mediate all access between subjects

and objects, be protected from modification, and be verifiable as correct."

The trusted computing based (TCB), as defined in AIO V5 (Harris) is: "all of the protection mechanisms within a computer system (software, hardware, and firmware) that are responsible for enforcing a security policy."

The security domain, "builds upon the definition of domain (a set of resources available to a subject) by adding the fact that resources withing this logical structure (domain) are working under the same security policy and managed by the

same group."

The following answers are incorrect:

"The security kernel" is incorrect. One of the places a reference monitor could be implemented is in the security kernel but this is not the best answer.

"The trusted computing base" is incorrect. The reference monitor is an important concept in the TCB but this is not the

best answer.

"The security domain is incorrect." The reference monitor is an important concept in the security domain but this is not the best answer.

Reference(s) used for this question:

Official ISC2 Guide to the CBK, page 324

AIO Version 3, pp. 272 - 274

AIOv4 Security Architecture and Design (pages 327 - 328) AIOv5 Security Architecture and Design (pages 330 - 331) Wikipedia article at https://en.wikipedia.org/wiki/Reference_monitor

QUESTION 34

Which of the following would be used to implement Mandatory Access Control (MAC)?

A. Clark-Wilson Access Control

B. Role-based access control

C. Lattice-based access control

D. User dictated access control

Correct Answer: C

Explanation: The lattice is a mechanism use to implement Mandatory Access Control (MAC)

Under Mandatory Access Control (MAC) you have:

Mandatory Access Control

Under-Non Discretionary Access Control (NDAC) you have:

Rule-Based Access Control

Role-Based Access Control

Under Discretionary Access Control (DAC) you have:

Discretionary Access Control

The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC,

DAC, Integrity level, File Permission, and more

For example in the case of MAC, if we look at common government classifications, we have the following:

TOP SECRET

SECRET ----------I am the user at secret CONFIDENTIAL

SENSITIVE BUT UNCLASSIFIED

UNCLASSIFIED

If you look at the diagram above where I am a user at SECRET it means that I can access document at lower classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements

are classification levels. My least upper bound is SECRET and my most lower bound is UNCLASSIFIED.

However the lattice could also be used for Integrity Levels such as:

VERY HIGH

HIGH

MEDIUM ----------I am a user, process, application at the medium level LOW

VERY LOW

In the case of Integrity levels you have to think about TRUST. Of course if I take for example the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a

process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is

an example of the Biba model.

Last but not least the lattice could be use for file permissions:

RWX

RW ---------User at this level

R

If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file because I do not have execute permission which is the X under Linux and UNIX. Many people confuse the Lattice Model and many books says MAC =

LATTICE, however the lattice can be use for other purposes.

There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that

dominates the object.

You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03

Also note that many book uses the same acronym for Role Based Access Control and Rule Based Access Control which is RBAC, this can be confusing. The proper way of writing the acronym for Rule Based Access Control is RuBAC,

unfortunately it is not commonly used.

There is a great article on technet that talks about the lattice in VISTA:

http://blogs.technet.com/b/steriley/archive/2006/07/21/442870aspx

also see:

KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 2: Access control systems (page 33).

and

http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

QUESTION 35

Multi-threaded applications are more at risk than single-threaded applications to

A. race conditions.

B. virus infection.

C. packet sniffing.

D. database injection.

Correct Answer: A

QUESTION 36

What is a common problem when using vibration detection devices for perimeter control?

A. They are vulnerable to non-adversarial disturbances.

B. They can be defeated by electronic means.

C. Signal amplitude is affected by weather conditions.

D. They must be buried below the frost line.

Correct Answer: A

Explanation: Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through.

They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.

Such sensors are proned to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lighting, it may trigger the alarm even thou there are no adversarial threat or

disturbance.

The following are incorrect answers:

All of the other choices are incorrect.

Reference used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496).

McGraw-Hill . Kindle Edition.

QUESTION 37

Object-Oriented Database (OODB) systems:

A. Are useful in storing and manipulating complex data, such as images and graphics.

B. Consume minimal system resources.

C. Are ideally suited for text-only information.

D. Require minimal learning time for programmers.

Correct Answer: A

The correct answer is "Are useful in storing and manipulating complex data, such as images and graphics". The other answers are false, because for answer "Are ideally suited for text-only information" relational databases are ideally suited to text-only information, "Require minimal learning time for programmers" and "Consume minimal system resources". OODB systems have a steep learning curve and consume a large amount of system resources.

QUESTION 38

Who can best decide what are the adequate technical security controls in a computer- based application system in regards to the protection of the data being used, the criticality of the data, and it\\'s sensitivity level?

A. System Auditor

B. Data or Information Owner

C. System Manager

D. Data or Information user

Correct Answer: B

Explanation: The data or information owner also referred to as "Data Owner" would be the best person. That is the individual or officer who is ultimately responsible for the protection of the information and can therefore decide what are the adequate security controls according to the data sensitivity and data criticality. The auditor would be the best person to determine the adequacy of controls and whether or not they are working as expected by the owner.

The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make

sure the organization complies with its own policies and the applicable laws and regulations. Organizations can have internal auditors and/ or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure

compliance is being met. For example CobiT, which is a model that most information security auditors follow when evaluating a security program. While many security professionals fear and dread auditors, they can be valuable tools in

ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problem.

The Official ISC2 Guide (OIG) says:

IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on

systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented,

operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Example:

Bob is the head of payroll. He is therefore the individual with primary responsibility over the payroll database, and is therefore the information/data owner of the payroll database. In Bob\\'s department, he has Sally and Richard working for him.

Sally is responsible for making changes to the payroll database, for example if someone is hired or gets a raise. Richard is only responsible for printing paychecks. Given those roles, Sally requires both read and write access to the payroll

database, but Richard requires only read access to it. Bob communicates these requirements to the system administrators (the "information/data custodians") and they set the file permissions for Sally\\'s and Richard\\'s user accounts so that

Sally has read/write access, while Richard has only read access. So in short Bob will determine what controls are required, what is the sensitivily and criticality of the Data. Bob will communicate this to the custodians who will implement the

requirements on the systems/DB. The auditor would assess if the controls are in fact providing the level of security the Data Owner expects within the systems/DB. The auditor does not determine the sensitivity of the data or the crititicality of

the data.

The other answers are not correct because:

A "system auditor" is never responsible for anything but auditing... not actually making control decisions but the auditor would be the best person to determine the adequacy of controls and then make recommendations.

A "system manager" is really just another name for a system administrator, which is actually an information custodian as explained above.

A "Data or information user" is responsible for implementing security controls on a day-to- day basis as they utilize the information, but not for determining what the controls should be or if they are adequate.

Official ISC2 Guide to the CISSP CBK, Third Edition , Page 477 Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition :

Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 294-298). Auerbach Publications. Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3108-3114).

Information Security Glossary

Responsibility for use of information resources

QUESTION 39

Of the multiple methods of handling risks which we must undertake to carry out business operations, which one involves using controls to reduce the risk?

A. Mitigation

B. Avoidance

C. Acceptance

D. Transference

Correct Answer: A

Explanation: Risk mitigation is the practice of the elimination of, or the significant decrease in the level of risk presented. Mitigating risk means you work around the risk with measures to reduce the risk. A good example could be a locked

down web server or firewall. You benefit from the service they provide but mitigate risks involved by technical measures.

Another example of risk mitigation can be seen in everyday life and are readily apparent in the information technology world. For example, to lessen the risk of exposing personal and financial information that is highly sensitive and confidential

organizations put countermeasures in place, such as firewalls, intrusion detection/prevention systems, and other mechanisms, to deter malicious outsiders from accessing this highly sensitive information.

Understand that conducting business in a computing world means assumption of risk. You have to make a management decision on whether to avoid, mitigate, transfer or simply accept it as a risk of doing business.

The following answers are incorrect:

Avoid: Risk with avoidance is when we eliminate the risk by avoiding it altogether. No surprise there but this answer is distinct from the others because you simply don\\'t undertake the risky process. It is incorrect here because you\\'re not

reducing the risk with controls as with mitigation.

Acceptance: This means that the risk is identified and understand and evaluated to be acceptable in order to conduct business operations. It is incorrect because you are accepting that the risk is present and conducting business anyhow but

don\\'t mitigate risk with controls like in the question here.

Transference: When we transfer risk, we pay someone else to undertake the risk on our behalf so that we may conduct operations and benefit from the risk but don\\'t undertake the risky operation ourselves. This is not the same as mitigation

so it is incorrect.

The following reference(s) was used to create this question:

Gregg, Michael; Haines, Billy (2012-02-16). CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware: Exam CAS-001 (p. 217-218). Wiley.

Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10183-10195). Auerbach Publications. Kindle Edition.

QUESTION 40

The Rijndael cipher employs a round transformation that is itself comprised of three layers of transformations. Which of the following is NOT one of these layers?

A. Non-linear mixing layer

B. Non-linear layer

C. Key addition layer

D. Linear mixing layer

Correct Answer: A

The correct answer is Non-linear mixing layer, a distracter.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.certbus.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: