QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

ISSMP Dumps
ISSMP Braindumps
ISSMP Real Questions
ISSMP Practice Test
ISSMP dumps free

ISC2

ISSMP

Information Systems Security Management(R) Professional

of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.
Answer option D is incorrect. A patent is a set of exclusive rights granted to anyone who invents any new and useful machine, process, composition of matter, etc. A patent enables the inventor to legally enforce his right to exclude others from using his invention.

Reference:
"http.//en.wikipedia.org/wiki/Trademark"

QUESTION: 216
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy
B. Backup policy
C. Privacy policy
D. User password policy

Answer: C

Explanation:
Monitoring the computer hard disks or e-mails of employees pertains to the privacy policy of an organization.
Answer option B is incorrect. The backup policy of a company is related to the backup of its data. Answer option A is incorrect. The network security policy is related to the security of a company's network.
Answer option D is incorrect. The user password policy is related to passwords that users provide to log on to the network.

QUESTION: 217
Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

A. No
B. Yes

Answer: B

Explanation:

Sarah is guilty under copyright laws because pleading ignorance of copyright infringement is not an excuse.What is copyright?
A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.

Reference:
"http.//en.wikipedia.org/wiki/Copyright"

QUESTION: 218
Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model
B. Bell-LaPadula Model
C. Biba Integrity Model
D. Access Matrix

Answer: A

Explanation:
The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable. The model represents a system as directed graph, where vertices are either subjects or objects. The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model. take and grant. They play a special role in the graph rewriting rules describing admissible changes of the graph.
Answer option D is incorrect. The access matrix is a straightforward approach that provides access rights to subjects for objects.
Answer option B is incorrect. The Bell-LaPadula model deals only with the confidentiality of classified material. It does not address integrity or availability.

QUESTION: 219
Which of the following plans is designed to protect critical business processes from natural or man- made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

A. Business continuity plan

B. Crisis communication plan
C. Contingency plan
D. Disaster recovery plan

Answer: A

Explanation:
The business continuity plan is designed to protect critical business processes from natural or man- made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes.Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.
Answer option B is incorrect. The crisis communication plan can be broadly defined as the plan for the exchange of information before, during, or after a crisis event. It is considered as a sub-specialty of the public relations profession that is designed to protect and defend an individual, company, or organization facing a public challenge to its reputation.
The aim of crisis communication plan is to assist organizations to achieve continuity of critical business processes and information flows under crisis, disaster or event driven circumstances.
Answer option C is incorrect. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.
Answer option D is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data.

Reference:
CISM Review Manual 2010, Contents. "Incident Management and Response"

QUESTION: 220
Which of the following concepts represent the three fundamental principles of information security?Each correct answer represents a complete solution. Choose three.

A. Confidentiality
B. Integrity
C. Availability

D. Privacy

Answer: A, B, C

Explanation:
The following concepts represent the three fundamental principles of information security.
1.Confidentiality
2.Integrity
3.Availability
Answer option C is incorrect. Privacy, authentication, accountability, authorization and identification are also concepts related to information security, but they do not represent the fundamental principles of information security.

Reference:
"http.//en.wikipedia.org/wiki/Information_security"

QUESTION: 221
Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

A. Shielding
B. Spoofing
C. Eavesdropping
D. Packaging

Answer: C

Explanation:
Eavesdropping is the process of listening in private conversations. It also includes attackers listening in on the network traffic. For example, it can be done over telephone lines (wiretapping), e-mail, instant messaging, and any other method of communication considered private.
Answer option B is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.
Answer option A is incorrect. Shielding cannot be done over e-mail and instant messaging. Shielding is a way of preventing electronic emissions that are generated from a computer or network from being used by unauthorized users for gathering confidential information. It minimizes the chances of eavesdropping within a network. Shielding can be provided by surrounding a computer room with a Farady cage. A Farady cage is a device that prevents

electromagnetic signal emissions from going outside the computer room. Shielding can also protect wireless networks from denial of service (DoS) attacks.Answer option D is incorrect. Packaging is a process in which goods are differentiated on the basis of the container in which they are stored, such as bottles, boxes, bags, etc.

Reference:
"http.//en.wikipedia.org/wiki/Eavesdropping"

QUESTION: 222
You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

A. Configuration identification
B. Physical configuration audit
C. Configuration control
D. Functional configuration audit

Answer: B

Explanation:
Physical Configuration Audit (PCA) is one of the practices used in Software Configuration Management for Software Configuration Auditing. The purpose of the software PCA is to ensure that the design and reference documentation is consistent with the as-built software product. PCA checks and matches the really implemented layout with the documented layout.
Answer option D is incorrect. Functional Configuration Audit or FCA is one of the practices used in Software Configuration Management for Software Configuration Auditing. FCA occurs either at delivery or at the moment of effecting the change. A Functional Configuration Audit ensures that functional and performance attributes of a configuration item are achieved.
Answer option C is incorrect. Configuration control is a procedure of the Configuration management. Configuration control is a set of processes and approval stages required to change a configuration item's attributes and to re-baseline them. It supports the change of the functional and physical attributes of software at various points in time, and performs systematic control of changes to the identified attributes.
Answer option A is incorrect. Configuration identification is the process of identifying the attributes that define every aspect of a configuration item. A configuration item is a product (hardware and/or software) that has an end-user purpose. These attributes are recorded in configuration documentation and baselined. Baselining an attribute forces formal configuration change control processes to be effected in the event that these attributes are changed.

QUESTION: 223
In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

A. Role-Based Access Control
B. Discretionary Access Control
C. Task-based Access Control
D. Mandatory Access Control

Answer: B

Explanation:
In the discretionary access control, an authority, within limitations, specifies what objects can be accessed by a subject.
Answer option D is incorrect. In the mandatory access control, a subject's access to an object is dependent on labels.
Answer option A is incorrect. In the role-based access control, a central authority determines what individuals can have access to which objects based on the individual's role or title in the organization.
Answer option C is incorrect. The task-based access control is similar to role-based access control, but the controls are based on the subject's responsibilities and duties.

Reference:
CISM Review Manual 2010, Contents. "Information Security Governance"

QUESTION: 224
Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution. Choose two.

A. Clark-Biba model
B. Clark-Wilson model
C. Bell-LaPadula model
D. Biba model

Answer: D, B

Explanation:
The Biba and Clark-Wilson access control models are used in the commercial sector. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped

into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.The Clark-Wilson security model provides a foundation for specifying and analyzing an integrity policy for a computing system.
Answer option C is incorrect. The Bell-LaPadula access control model is mainly used in military systems.
Answer option A is incorrect. There is no such access control model as Clark-Biba.

Reference:
"http.//en.wikipedia.org/wiki/Biba"