**Vendor: ISC2**

**Exam Code: CISSP**

**Exam Name: Certified Information Systems Security Professional**

**QUESTION 1**
Susan, an attorney, has been hired to fill a new position at Widgets Inc. The position is Chief Privacy Officer (CPO). What is the primary function of her new role?

A. Ensuring the protection of partner data
B. Ensuring the accuracy and protection of company financial information
C. Ensuring that security policies are defined and enforced
D. Ensuring the protection of customer, company, and employee data

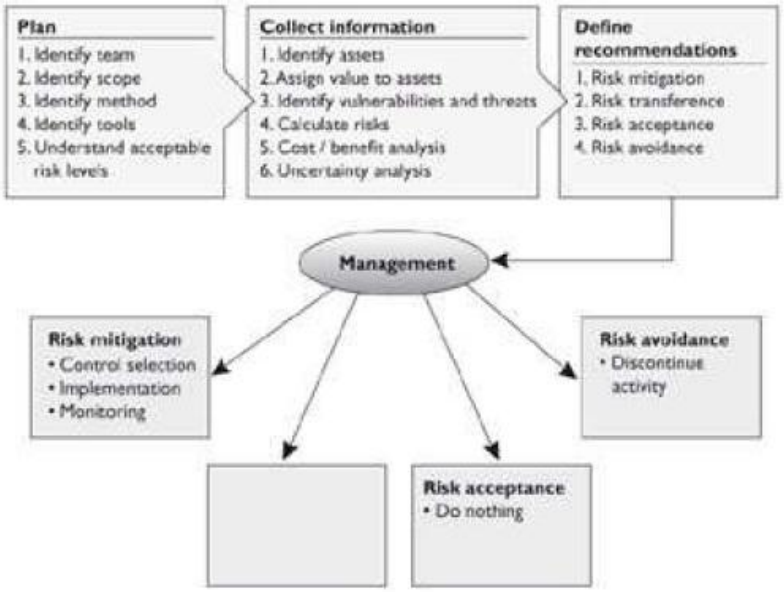
**Answer:** D

**QUESTION 2**
Risk assessment has several different methodologies. Which of the following official risk methodologies was not created for the purpose of analyzing security risks?

A. FAP
B. OCTAVE
C. ANZ 4360
D. NIST SP 800-30

**Answer:** C

**QUESTION 3**
There are four ways of dealing with risk. In the graphic that follows, which method is missing and what is the purpose of this method?




A. Risk transference. Share the risk with other entities.
B. Risk reduction. Reduce the risk to an acceptable level.
C. Risk rejection. Accept the current risk.
D. Risk assignment. Assign risk to a specific owner.

**QUESTION 4**

Which of the following statements correctly describes biometric methods?

A. They are the least expensive and provide the most protection.
B. They are the most expensive and provide the least protection.
C. They are the least expensive and provide the least protection.
D. They are the most expensive and provide the most protection.

**Answer:** D

**QUESTION 5**

What is the reason for enforcing the separation of duties?

A. No one person can complete all the steps of a critical activity.
B. It induces an atmosphere for collusion.

C. It increases dependence on individuals.
D. It makes critical tasks easier to accomplish.

**Answer:** A

**QUESTION 6**
Which access control policy is enforced when an environment uses a nondiscretionary model?

A. Rule-based
B. Role-based
C. Identity-based
D. Mandatory

**Answer:** B

**QUESTION 7**
If a company has a high turnover rate, which access control structure is best?

A. Role-based
B. Decentralized
C. Rule-based
D. Discretionary

**Answer:** A

**QUESTION 8**
Which of the following is not part of user provisioning?

A. Creation and deactivation of user accounts
B. Business process implementation
C. Maintenance and deactivation of user objects and attributes
D. Delegating user administration

**Answer:** B

**QUESTION 9**
What is the difference between password cracking and password guessing?

A. They are the same
B. Password guessing attempts to log into the system, password cracking attempts to determine a password used to create a hash
C. Password guessing uses salts, password cracking does not
D. Password cracking risks account lockout, password guessing does not

**Answer:** B

**QUESTION 10**
Within Kerberos, which part is the single point of failure?

A. The Ticket Granting Ticket
B. The Realm
C. The Key Distribution Center
D. The Client-Server session key

**Answer:** C

**QUESTION 11**
A potential vulnerability of the Kerberos authentication server is

A. Single point of failure
B. Asymmetric key compromise
C. Use of dynamic passwords
D. Limited lifetimes for authentication credentials

**Answer:** A

**QUESTION 12**
What is the best description of a security kernel from a security point of view?

A. Reference monitor
B. Resource manager
C. Memory mapper
D. Security perimeter

**Answer:** A

**QUESTION 13**
Virtual storage combines RAM and secondary storage for system memory. Which of the following is a security concern pertaining to virtual storage?

A. More than one process uses the same resource.
B. It allows cookies to remain persistent in memory.
C. It allows for side-channel attacks to take place.
D. Two processes can carry out a denial-of-service.

**Answer:** A

**QUESTION 14**
The trusted computing base (TCB) ensures security within a system when a process in one domain must access another domain in order to retrieve sensitive information. What function does the TCB initiate to ensure that this is done in a secure manner?

A. I/O operational execution
B. Process deactivation
C. Execution domain switching
D. Virtual memory to real memory mapping

**Answer:** C

**QUESTION 15**
Bethany is working on a mandatory access control (MAC) system. She has been working on a file that was classified as Secret. She can no longer access this file because it has been reclassified as Top Secret. She deduces that the project she was working on has just increased in confidentiality and she now knows more about this project than her clearance and need-to-know allows. Which of the following refers to a concept that attempts to prevent this type of scenario from occurring?

A. Covert storage channel
B. Inference attack
C. Noninterference
D. Aggregation

**Answer:** C

**QUESTION 16**
Operating systems can be programmed to carry out different methods for process isolation. Which of the following refers to a method in which an interface defines how communication can take place between two processes and no process can interact with the other's internal programming code?

A. Virtual mapping
B. Encapsulation of objects
C. Time multiplexing
D. Naming distinctions

**Answer:** B

**QUESTION 17**
The Information Technology Infrastructure Library (ITIL) consists of five sets of instructional books. Which of the following is considered the core set and focuses on the overall planning of the intended IT services?

A. Service Operation

B. Service Design

C. Service Transition

D. Service Strategy

**Answer:** D

**QUESTION 18**

There are five different classes of fire. Each depends upon what is on fire. Which of the following is the proper mapping for the items missing in the provided table?

| Fire class | Type of fire | Elements of fire | Suppression method |
|---|---|---|---|
| Class A | | | Water, soda acid |
| Class B | | | $C0_2$ FM-200 |
| Class C | | | Gas (Halon) or $C0_2$ nonconductive extinguishing agent |
| Class D | | | Dry chemicals |
| Class K | | | A wet chemical |

A. Class D—combustible metals

B. Class C—liquid

C. Class B—electrical

D. Class A—electrical

**Answer:** A

**QUESTION 19**

Which of the following best describes Ethernet transmissions over a LAN?

A. Traffic is sent to a gateway that sends it to the destination system.

B. Traffic is bursty in nature and broadcasts data to all hosts on the subnet.

C. Traffic streams and does not broadcast data.

D. Traffic is contained within collision domains but not broadcast domains.

**Answer:** B

**QUESTION 20**

Which of the following protocols work in the following layers: application, data link, network, and transport?

A. FTP, ARP, TCP, and UDP
B. FTP, ICMP, IP, and UDP
C. TFTP, ARP, IP, and UDP
D. TFTP, RARP, IP, and ICMP

**Answer:** C