Vendor:ISC

Exam Code:CISSP

Exam Name: Certified Information Systems Security Professional

Version: Demo

QUESTION 1

If a content management system (CSM) is implemented, which one of the following would occur?

A. The test and production systems would be riming the same software

B. The applications placed into production would be secure

C. Developers would no longer have access to production systems

D. Patching the systems would be completed mere quickly

Correct Answer: A

QUESTION 2

How should the retention period for an organization\\'s social media content be defined?

A. By the retention policies of each social media service

B. By the records retention policy of the organization

C. By the Chief Information Officer (CIO)

D. By the amount of available storage space

Correct Answer: B

QUESTION 3

One of Canada\\'s leading pharmaceutical firms recently hired a Chief Data Officer (CDO) to oversee its data privacy program. The CDO has discovered the firm\\'s marketing department has been collecting information from individuals without their knowledge and consent via the company website. Which of the following privacy regulations should concern the CDO regarding this practice?

A. The Health Insurance Portability and Accountability Act (HIPAA)

B. The Privacy Act of 1974

C. The Fair Information Practice Principles (FIPPs)

D. The Personal Information Protection and Electronic Documents Act (PIPEDA)

Correct Answer: D

QUESTION 4

An organization has requested storage area network (SAN) disks for a new project. What Redundant Array of Independent Disks (RAID) level provides the BEST redundancy and fault tolerance?

A. RAID level 1

B. RAID level 3

C. RAID level 4

D. RAID level 5

Correct Answer: D

QUESTION 5

Which of the following analyses is performed to protect information assets?

A. Business impact analysis

B. Feasibility analysis

C. Cost benefit analysis

D. Data analysis

Correct Answer: A

QUESTION 6

Which concept might require users to use a second access token or to re-enter passwords to gain elevated access rights in the identity and access provisioning life cycle?

A. Time-based

B. Enrollment

C. Least privilege

D. Access review

Correct Answer: B

QUESTION 7

Which of the following has the GREATEST Impact on an organization\\'s security posture?

A. Audit findings related to employee access and permissions process

B. International and country-specific compliance requirements

C. Security violations by employees and contractors

D. Resource constraints due to increasing costs of Supporting security

Correct Answer: B

QUESTION 8

A vendor released a security patch for a dangerous vulnerability affecting thousands of computers in an organization. Which of the following actions will the security practitioner do FIRST to mitigate the security risk?

A. Deploy the patch.

B. Accept the risk.

C. Transfer the risk.

D. Evaluate the patch.

Correct Answer: D

Reference: https://its.ucsc.edu/security/breaches.html

QUESTION 9

A web-based application known to be susceptible to attacks is now under review by a senior developer. The organization would like to ensure this application Is less susceptible to injection attacks specifically,

What strategy will work BEST for the organization\\'s situation?

A. Do not store sensitive unencrypted data on the back end.

B. Whitelist input and encode or escape output before it is processed for rendering.

C. Limit privileged access or hard-coding logon credentials,

D. Store sensitive data in a buffer that retains data in operating system (OS) cache or memory.

Correct Answer: B

QUESTION 10

During the risk assessment phase of the project the CISO discovered that a college within the University is collecting Protected Health Information (PHI) data via an application that was developed in-house. The college collecting this data is fully aware of the regulations for Health Insurance Portability and Accountability Act (HIPAA) and is fully compliant.

What is the best approach for the CISO?

A. Document the system as high risk

B. Perform a vulnerability assessment

C. Perform a quantitative threat assessment

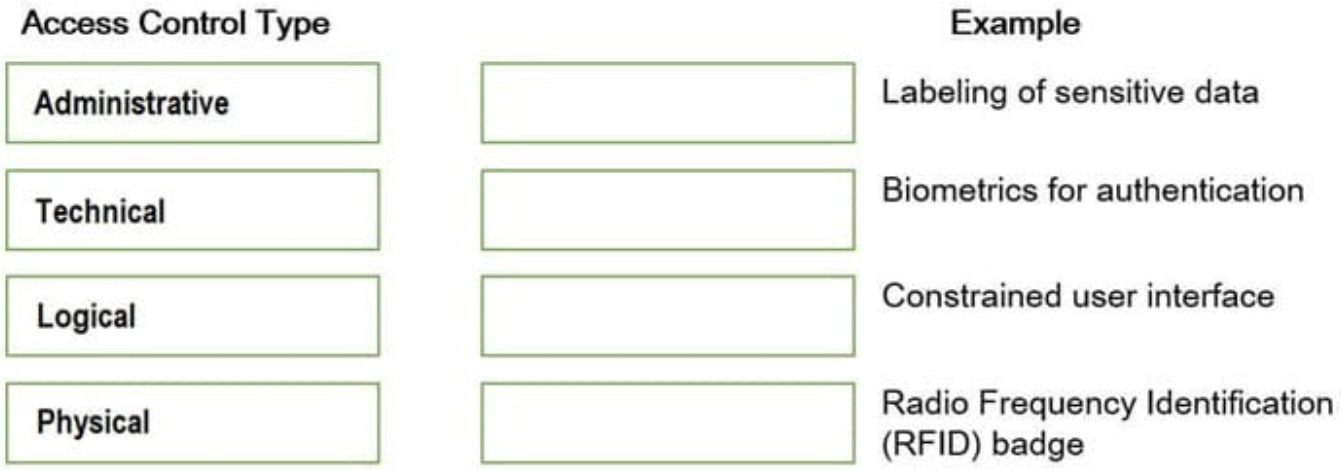
D. Notate the information and move on

Correct Answer: B

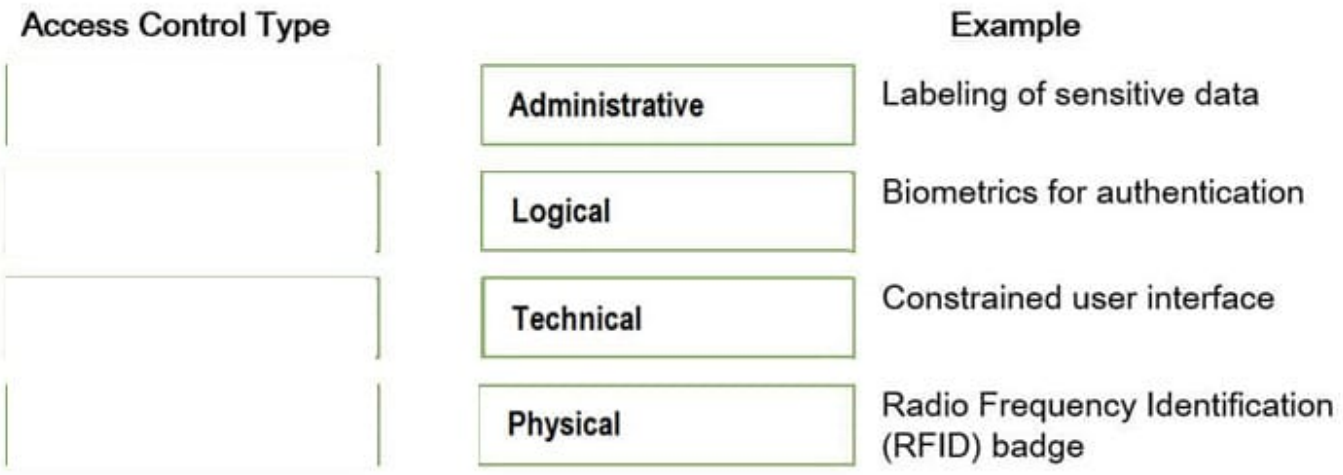
QUESTION 11

Match the access control type to the example of the control type. Drag each access control type net to its corresponding example.

Select and Place:



Correct Answer:



QUESTION 12

When using Security Assertion markup language (SAML), it is assumed that the principal subject

A. accepts persistent cookies from the system.

B. allows Secure Sockets Layer (SSL) for data exchanges.

C. is on a system that supports remote authorization.

D. enrolls with at least one identity provider.

Correct Answer: D