# Question 1

Question Type: **MultipleChoice**

Which of the following is MOST likely to be included in an enterprise information security policy?

## Options:

**A)** Password composition requirements

**B)** Consequences of noncompliance

**C)** Audit trail review requirements

**D)** Security monitoring strategy

## Answer:

B

# Question 2

Question Type: **MultipleChoice**

Which of the following metrics BEST evaluates the completeness of disaster-recovery preparations?

## Options:

**A)** Ratio of successful to unsuccessful tests

**B)** Number of published application-recovery plans

**C)** Ratio of recovery-plan documents to total applications

**D)** Ratio of tested applications to total applications

## Answer:

A

# Question 3

**Question Type:** **MultipleChoice**

An organization's marketing department has requested access to cloud-based collaboration sites for exchanging media files with external marketing companies. As a result, the information security manager has been asked to perform a risk assessment. Which of the following should be the MOST important consideration?

## Options:

**A)** Methods for transferring the information

**B)** The security of the third-party cloud provider

**C)** Reputations of the external marketing companies

**D)** The information to be exchanged

## Answer:

D

# Question 4

**Question Type:** **MultipleChoice**

Which of the following would provide senior management with the BEST overview of the performance of information security risk treatment options?

## Options:

**A)** Before-and-after heat maps

**B)** Analysis of recent incident

**C)** Detailed risk analysis of the treatments

**D)** individual risk assessments

## Answer:

A

# Question 5

**Question Type: MultipleChoice**

Which of the following is MOST likely to result from a properly conducted post-incident review?

## Options:

**A)** Breach information is provided to the organization's key stakeholders and users.

**B)** The cause of the incident is discovered and remediated.

**C)** Forensic evidence is reviewed and provided to law enforcement

**D)** The incident response team discovers inefficiencies in the recovery process.

**Answer:**

D

# Question 6

**Question Type:** **MultipleChoice**

Which of the following is the BEST indication that a recently adopted information security framework is a good fit for an organization?

**Options:**

**A)** The framework includes industry-recognized information security best practices.

**B)** The number of security incidents has significantly declined

**C)** The business has obtained framework certification.

**D)** Objectives in the framework correlate directly to business practices

**Answer:**

D

# Question 7

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

## Options:

**A)** Redundant

**B)** Shared

**C)** Warm

**D)** Mobile

## Answer:

A

# Question 8

A message is being sent with a hash. The risk of an attacker changing the message and generating an authentic hash value c*n be mitigated by:

## Options:

**A)** generating hash output that is the same size as the original message,

**B)** requiring the recipient to use a different hash algorithm,

**C)** using the senders public key to encrypt the message.

**D)** using a secret key m conjunction with the hash algorithm.

## Answer:

D

**To Get Premium Files for CISM Visit**

**For More Free Questions Visit**

**20% DISCOUNT**