

BCS

CISMP-V9 Exam

**BCS Foundation Certificate in Information Security Management
Principles V9.0**

**Questions & Answers
Demo**

Version: 4.0

Question: 1

Which of the following is NOT an accepted classification of security controls?

- A. Nominative.
- B. Preventive.
- C. Detective.
- D. Corrective.

Answer: A

Question: 2

Which three of the following characteristics form the AAA Triad in Information Security?

- 1. Authentication
 - 2. Availability
 - 3. Accounting
 - 4. Asymmetry
 - 5. Authorisation
-
- A. 1, 2 and 3.
 - B. 2, 4, and 5.
 - C. 1, 3 and 4.
 - D. 1, 3 and 5.

Answer: D

Question: 3

According to ISO/IEC 27000, which of the following is the definition of a vulnerability?

- A. A weakness of an asset or group of assets that can be exploited by one or more threats.
- B. The impact of a cyber attack on an asset or group of assets.
- C. The threat that an asset or group of assets may be damaged by an exploit.
- D. The damage that has been caused by a weakness in a system.

Answer: A

Vulnerability

A vulnerability is a weakness of an asset or control that could potentially be exploited by one or more threats.

An asset is any tangible or intangible thing or characteristic that has value to an organization, a control is any administrative, managerial, technical, or legal method that can be used to modify or manage risk, and a threat is any potential event that could harm an organization or system.

<https://www.praxiom.com/iso-27000-definitions.htm>

Question: 4

Which term describes the acknowledgement and acceptance of ownership of actions, decisions, policies and deliverables?

- A. Accountability.
- B. Responsibility.
- C. Credibility.
- D. Confidentiality.

Answer: A

https://hr.nd.edu/assets/17442/behavior_model_4_ratings_3_.pdf

Question: 5

Which security concept provides redundancy in the event a security control failure or the exploitation of a vulnerability?

- A. System Integrity.
- B. Sandboxing.
- C. Intrusion Prevention System.
- D. Defence in depth.

Answer: D

[https://en.wikipedia.org/wiki/Defense_in_depth_\(computing\)](https://en.wikipedia.org/wiki/Defense_in_depth_(computing))