

# DUMPS ARENA

Information Security Foundation (based on  
ISO/IEC 27002) (EX0-105)

Exin ISFS

Version Demo

Total Demo Questions: 10

Total Premium Questions: 80

Buy Premium PDF

<https://dumpsarena.co>

[sales@dumpsarena.co](mailto:sales@dumpsarena.co)

sales@dumpsarena.co  
dumpsarena.co

**QUESTION NO: 1**

Your company has to ensure that it meets the requirements set down in personal data protection legislation. What is the first thing you should do?

- A. Make the employees responsible for submitting their personal data.
- B. Translate the personal data protection legislation into a privacy policy that is geared to the company and the contracts with the customers.
- C. Appoint a person responsible for supporting managers in adhering to the policy.
- D. Issue a ban on the provision of personal information.

**ANSWER: B****QUESTION NO: 2**

What do employees need to know to report a security incident?

- A. How to report an incident and to whom.
- B. Whether the incident has occurred before and what was the resulting damage.
- C. The measures that should have been taken to prevent the incident in the first place.
- D. Who is responsible for the incident and whether it was intentional.

**ANSWER: A****QUESTION NO: 3**

You are the first to arrive at work in the morning and notice that the CD ROM on which you saved contracts yesterday has disappeared. You were the last to leave yesterday. When should you report this information security incident?

- A. This incident should be reported immediately.
- B. You should first investigate this incident yourself and try to limit the damage.
- C. You should wait a few days before reporting this incident. The CD ROM can still reappear and, in that case, you will have made a fuss for nothing.

**ANSWER: A**

**QUESTION NO: 4**

You work for a large organization. You notice that you have access to confidential information that you should not be able to access in your position. You report this security incident to the helpdesk. The incident cycle is initiated. What are the stages of the security incident cycle?

- A. Threat, Damage, Incident, Recovery
- B. Threat, Damage, Recovery, Incident
- C. Threat, Incident, Damage, Recovery
- D. Threat, Recovery, Incident, Damage

**ANSWER: C****QUESTION NO: 5**

What is a repressive measure in the case of a fire?

- A. Taking out fire insurance
- B. Putting out a fire after it has been detected by a fire detector
- C. Repairing damage caused by the fire

**ANSWER: B****QUESTION NO: 6**

Why do organizations have an information security policy?

- A. In order to demonstrate the operation of the Plan-Do-Check-Act cycle within an organization.
- B. In order to ensure that staff do not break any laws.
- C. In order to give direction to how information security is set up within an organization.
- D. In order to ensure that everyone knows who is responsible for carrying out the backup procedures.

**ANSWER: C****QUESTION NO: 7**

You have a small office in an industrial area. You would like to analyze the risks your company faces. The office is in a pretty remote location; therefore, the possibility of arson is not entirely out of the question. What is the relationship between the threat of fire and the risk of fire?

- A. The risk of fire is the threat of fire multiplied by the chance that the fire may occur and the consequences thereof.
- B. The threat of fire is the risk of fire multiplied by the chance that the fire may occur and the consequences thereof.

**ANSWER: A**

#### QUESTION NO: 8

Why is compliance important for the reliability of the information?

- A. Compliance is another word for reliability. So, if a company indicates that it is compliant, it means that the information is managed properly.
- B. By meeting the legislative requirements and the regulations of both the government and internal management, an organization shows that it manages its information in a sound manner.
- C. When an organization employs a standard such as the ISO/IEC 27002 and uses it everywhere, it is compliant and therefore it guarantees the reliability of its information.
- D. When an organization is compliant, it meets the requirements of privacy legislation and, in doing so, protects the reliability of its information.

**ANSWER: B**

#### QUESTION NO: 9

You read in the newspapers that the ex-employee of a large company systematically deleted files out of revenge on his manager. Recovering these files caused great losses in time and money.

What is this kind of threat called?

- A. Human threat
- B. Natural threat
- C. Social Engineering

**ANSWER: A**

#### QUESTION NO: 10

What is the goal of an organization's security policy?

- A. To provide direction and support to information security
- B. To define all threats to and measures for ensuring information security
- C. To document all incidents that threaten the reliability of information

D. To document all procedures required to maintain information security

**ANSWER: A**