Download CertiProf I27001F Exam Dumps Free

Shared by Gill on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What details must be included in a Statement of Applicability?

Options:

A- A list of the risks applicable to the organization
B- Evidence of top management authorization of the controls
C- The necessary controls with justification for inclusion and exclusion
D- The information security policy

Answer:

C

Explanation:

The Statement of Applicability is a documented result of the risk treatment process. It must include the necessary controls and justification for their inclusion, whether the controls are implemented, and justification for excluding controls from Annex A when they are not applicable. It does not need to be a list of risks, proof of management authorization, or the policy itself. Therefore, option C is correct.

=======

Question 2

Question Type: MultipleChoice

The information security policy must be known by:

Options:

A- The quality management representative
B- The IT Manager
C- The IT Security Manager
D- Everyone in the organization

Answer:

D

Explanation:

ISO/IEC 27001:2022 requires the information security policy to be available as documented information, communicated within the organization, and available to interested parties as appropriate. In practical terms, this means the policy must be communicated to relevant persons in the organization so they understand the direction and expectations related to information security. Among the options provided, the best and correct answer is D, because the policy is intended to be known broadly across the organization, not restricted to a single role or department.

Question 3

Question Type: MultipleChoice

In the context of clause 6.1 actions to address risks and opportunities, What is defined as residual risk?

Options:

A- Effect of uncertainty on objectives
B- Informed decision to take a particular risk
C- Risk remaining after risk treatment
D- Establishing and maintaining information security risk criteria

Answer:

C

Explanation:

Residual risk is the risk that remains after risk treatment has been applied. In an ISMS, organizations assess risks, select treatment options, and implement controls or other measures to reduce risk to an acceptable level. Even after treatment, some level of risk may still remain, and that remaining portion is called residual risk. Therefore, option C is correct.

=======

Question 4

Question Type: MultipleChoice

During the operation of the ISMS, what is a requirement for information security objectives?

Options:

A- Develop improvement plans using ISO/IEC 27002 to achieve the information security objectives
B- Maintain documented information about the objectives
C- Ensure that the objectives are consistent with the information security policy
D- Establish objectives for relevant functions and levels

Answer:

C

Explanation:

ISO/IEC 27001:2022 requires information security objectives to be established at relevant functions and levels, to be consistent with the information security policy, to be measurable if practicable, and to be monitored, communicated, and updated as appropriate. It also requires documented information on the objectives. Among the answer choices, option C is the best single answer because it expresses one of the core mandatory characteristics of the objectives. Even though options B and D are also requirements, the question asks for one answer only, and option C is the most fundamental wording in the set.

=======

Question 5

Question Type: MultipleChoice

What are the phases of the PDCA cycle?

Options:

A- Plan, Validate, Verify, Act
B- Plan, Do, Check, Act
C- Plan, Do, Verify, Assure
D- Propose, Do, Validate, Act

Answer:

B

Explanation:

The PDCA cycle stands for Plan, Do, Check, Act. It is a management model commonly associated with management systems, including the implementation and continual improvement of an ISMS. In the context of ISO/IEC 27001:2022, this logic supports planning the ISMS, implementing and operating it, monitoring and reviewing performance, and taking actions for continual improvement. Therefore, option B is correct.

=======

Question 6

Question Type: MultipleChoice

How should top management provide evidence of its commitment to the Information Security Management System?

Options:

A- By communicating the importance of meeting ISMS requirements
B- By conducting an annual internal audit of the Information Security Management System
C- By operating the Information Security Management System once it has been established
D- By defining a risk assessment approach

Answer:

A

Explanation:

One of the explicit leadership responsibilities in ISO/IEC 27001:2022 is for top management to

communicate the importance of effective information security management and of conforming to the ISMS requirements. This communication helps demonstrate visible commitment and organizational direction. Conducting internal audits and defining the risk assessment approach are important activities within the ISMS, but they are not the best direct expression of top management's evidence of commitment among the options listed. Therefore, option A is correct.

=======