Vendor: PECB

Exam Code: ISO-IEC-27001-Foundation

Exam Name: ISO/IEC 27001 (2022) Foundation

Version: DEMO

QUESTION 1
What is required to be reported by the Information security event reporting control?

A. Information disclosure
B. Unauthorized access
C. Asset disposal
D. Observed or suspected events

Answer: D
Explanation:
Annex A, control 6.8 (Information security event reporting) specifies:

"Information security events should be reported through appropriate management channels as quickly as possible. The organization should require all employees and contractors to note and report any observed or suspected information security events."

QUESTION 2
Which action is a required response to an identified residual risk?

A. By default, it shall be controlled by information security awareness and training
B. Top management shall delegate its treatment to risk owners
C. It shall be reviewed by the risk owner to consider acceptance
D. The organization shall change practices to avoid the risk occurring

Answer: C
Explanation:
Clause 6.1.3 (e) specifies:

"The organization shall obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks."

This confirms that residual risks -- those remaining after risk treatment -- must be reviewed and formally accepted by the designated risk owner.

QUESTION 3
Which statement describes the Classification of information control in Annex A of ISO/IEC 27001?

A. Ensures that all information assets are labelled with their classification
B. Ensures that information is classified based on confidentiality, integrity and availability
C. Ensures that security perimeters are used to protect assets
D. Ensures the rules to control physical and logical access apply to assets

Answer: B
Explanation:
Annex A.5.12 (Classification of information) states:

"Information should be classified according to the information security needs of the organization based on confidentiality, integrity and availability."

QUESTION 4
Identify the missing word(s) in the following sentence.

"Information security, cybersecurity and privacy protection ?[?]" is the title of ISO/IEC 27005.

A. Guidelines for information security management systems auditing
B. Information security management systems ?Requirements
C. Guidance on managing information security risks
D. Information security controls

Answer: C
Explanation:
ISO/IEC 27005:2022 is titled:

"Information security, cybersecurity and privacy protection -- Guidance on managing information security risks."

This standard provides structured methodologies for identifying, analyzing, evaluating, and treating risks, in alignment with ISO/IEC 27001's risk management requirements (Clause 6.1.2 and 6.1.3). It supports organizations in implementing the risk management process that underpins an ISMS.

QUESTION 5
Which activity is an operational planning and control requirement?

A. Review the consequences of unintended changes
B. Perform information security risk assessments at planned intervals
C. Scheduling of second party audits
D. Document information security objectives

Answer: A
Explanation:
Clause 8.1 (Operational planning and control) requires organizations to:

"Ensure that changes are controlled. The organization shall review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary."

This requirement ensures that operational processes are planned, controlled, and adjusted where unexpected changes occur.

QUESTION 6
Which aspect of ISO/IEC 27001 requires that contractors know about the organization's information security policies?

A. Nonconformity and corrective action
B. Competence
C. Communication
D. Awareness

Answer: D
Explanation:

Clause 7.3 (Awareness) requires:

"Persons doing work under the organization's control shall be aware of: (a) the information security policy; (b) their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance; (c) the implications of not conforming with the ISMS requirements."

QUESTION 7
Identify the missing word(s) in the following control relating to the Policies for information security control.

"Information security policy and topic-specific policies should be defined, approved by management, [?] and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur."

A. published
B. established and maintained
C. published, communicated to
D. communicated to

Answer: C
Explanation:
Annex A.5.1 (Policies for information security) states:

"Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur."

This confirms that the missing words are "published, communicated to." The control emphasizes not just defining and approving policies but ensuring they are actively distributed and communicated so that relevant stakeholders are aware of and acknowledge them.

QUESTION 8
Which benefit is NOT relevant by implementing an ISMS for an organization?

A. Information security compliance will increase stakeholder trust in the organization
B. Information security staff will be qualified to ISO/IEC 27001 Foundation level
C. Information security controls are tailored to suit the organization's specific circumstances
D. Information security risks are assessed and the probability and/or impact reduced

Answer: B
Explanation:
The benefits of implementing an ISMS under ISO/IEC 27001 are well established. Clause 0.1 (General) explains that an ISMS provides a systematic approach to managing sensitive information and "preserves confidentiality, integrity, and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed."

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**