Question sheet

Name: ______________________________

ID number: ______________________________

Signature: ______________________________

In order to receive the ISMS 27001 Foundation Examination Certificate, the examination passed in the multiple-choice procedure must be successfully passed.

Version: ISO/IEC 27001:2013 + Cor. 1:2014

Language: English

Duration: 45 minutes

Format: 30 multiple-choice questions; with two or three response possibilities, one, two or all three responses can be correct.

Minimum points: 20 of 30

Each completely correctly answered question gives a point. In the case of incorrectly answered questions, there are 0 points (but no point deduction). A wrong question is answered if a wrong answer is marked, or not all correct ones have been checked.

Aid for completing the answer form:

How do I mark correctly?
For this test, you will receive a questionnaire and a reply form. The answers must be made by means of appropriate markings on the answer sheet. This is evaluated by machine, and handwritten notes are not taken into account. Checkboxes on the questionnaire are not evaluated! For your markings, use only a black or blue ballpoint pen of normal character. The markings must be clearly and precisely positioned through a cross. If you want to correct a check, fill the checkbox completely, which means that this checkbox is evaluated as an empty check box. A new correction is then no longer possible!

Completion of the matriculation number:
At the beginning of the exam, enter your 9-digit matriculation number on the answer sheet in the field provided for this purpose. Then transfer your matriculation number to the boxes below, which are numbered from 0 to 9. The first column corresponds to the 1st digit of your matriculation number, the second column corresponds to the 2nd digit of your matriculation number, etc.

Transferring the right group:
Please transfer the group you find in the questionnaire header to the corresponding field on the answer sheet.

Good luck on the exam!

1) What is correct with respect to the PDCA cycle?

a) PDCA describes the characteristics of information to be maintained in the context of information security.
b) The structure of the ISO/IEC 27001 standard is based, at least in parts, on the PDCA approach.
c) P stands for "Plan", D for "Do", C for "Check" and A for "Act".

2) According to the section "context of the organization" of ISO/IEC 27001, which of the following activities are required?

a) Determine the requirements of interested parties relevant to information security
b) Establish organizational responsibilities for suppliers in collaboration with administrative units
c) Determine the interested parties that are relevant to the ISMS

3) What do persons need to be aware of when doing work under the control of an organization that claims conformity against ISO/IEC 27001?

a) The implications of not conforming with the ISMS requirements
b) All information security risk treatment actions according to the risk treatment plan
c) Their contribution to the effectiveness of the ISMS

4) What is correct with respect to the ISO/IEC 27001 standard?

a) The standard specifies requirements for bodies providing audit and certification of information security management systems.
b) The standard defines requirements for an information security management system (ISMS).
c) The standard is part of a larger family of standards.

5) Which of the following standards from the ISO/IEC 27000 family contain general, non-sector-specific, guidelines?

a) ISO/IEC 27006
b) ISO/IEC 27019
c) ISO/IEC 27002

6) Which of the following statements are correct with respect to controls?

a) All measures formulated in ISO / IEC 27001 Annex A are of a purely organizational nature
b) Controls may cover processes and policies.
c) All controls formulated in ISO/IEC 27001 (Annex A) are of a technical nature.

7) According to ISO/IEC 27001, what must an organization do as part of their information security risk treatment process?

a) Formulate an information security risk treatment plan
b) Evaluate information security risks
c) Determine the controls that are necessary to implement the information security risk treatment option(s) chosen

8) Which are the steps that need to be defined and implemented as part of the information security risk assessment process?

a) Identify information security risks
b) Avoid information security risks
c) Treat Information security risks

9) According to ISO/IEC 27001, section "Support" (7), what shall an organization do to effectively establish and operate an ISMS?

a) Ensure that the security officer has released and approved the information security policy
b) Determine and maintain necessary documentation
c) Ensure that relevant persons are aware of their contribution to the effectiveness of the ISMS

10) Which of the following steps need to be performed (among others) by an organization to introduce, maintain, and / or improve an ISMS?

a) Identification of information assets and related information security requirements (required level of protection)
b) Reporting of serious information security incidents to supervisory authorities
c) Distribution of the risk treatment plan to all interested parties

11) According to ISO/IEC 27001, section "Leadership" (5), which of the following activities are required by top management to demonstrate their accountability for and commitment to information security and the ISMS?

a) Attend all meetings of the computer emergency response team (CERT)
b) Ensure that the resources needed for the ISMS are available
c) Ensure that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization

12) What is confidentiality?

a) Property that information is well-known and communicated
b) Property hat an entity is what it claims to be
c) Property that information is not made available or disclosed to unauthorized individuals

13) What should internal ISMS audits provide information about?

a) Whether the ISMS meets the organization's requirements.
b) Whether the ISMS is being effectively implemented and maintained.
c) Which information security incidents could have been avoided.

14) ISO/IEC 27001 defines control objectives and controls for ...

a) Asset management
b) Human resource security
c) Physical and environmental security

15) While operating an ISMS according to ISO/IEC 27001, which of the following activities are required in connection with managing information security risks?

a) Risk assessments shall be carried out at planned intervals.
b) Every risk assessment shall be followed by a management review of the ISMS.
c) A risk assessment shall be carried out when significant changes are about to occur.

16) Which of the following frameworks, standards, or standard families are primarily concerned with IT or information security (or are referred to as IT or information security standards)?

a) FitSM
b) ISO/IEC 27000
c) ISIS12

17) Which of the following activities would top management carry out to demonstrate their engagement in connection with an ISMS?

a) Assess all information security risks
b) Show clear commitment to information security objectives
c) Conduct audit interviews with all employees

18) Which of the following statements are correct with respect to ISO/IEC 27001, Annex A?

a) Annex A is normative, and where exclusions are made, they must be justified.
b) Annex A defines control objectives for information security.
c) Annex A is a catalog of security threats.

19) What is correct with respect to controls in the context of the ISO/IEC 27000 standard?

a) In Annex A of the ISO/IEC 27001 standard, each control refers to one or more control objectives.
b) ISO/IEC 27002 covers the same set of controls as defined in Annex A of ISO/IEC 27001.
c) Controls are defined in Annex A of the ISO/IEC 27001 standard.

20) Which of the following situations reflect a violation of integrity?

a) Information in a document was made available to an unauthorized individual.
b) Information was added to a document by an unauthorized individual.
c) A document has not been encrypted.

21) What must be subject to continual improvement according to ISO/IEC 27001, section "Improvement" (10)?

a) The lawfulness of the ISMS
b) The effectiveness of the ISMS
c) The accuracy of the ISMS

22) What are the criteria that must be defined and applied as part of the information security risk assessment process according to ISO/IEC 27001?

a) Criteria for performing assessments of risk treatment actions
b) Risk acceptance criteria
c) Risk documentation criteria

23) Which of the following statements are correct with respect to Annex A of ISO/IEC 27001, in particular in the context of information security risk treatment?

a) Annex A contains a scope statement that must be adopted by all organizations that claim conformity against ISO/IEC 27001.
b) Annex A contains a comprehensive list of control objectives and controls.
c) Annex A provides an overview of the most relevant information security threats that need to be considered when assessing information security risks.

24) An audit is a process intended to determine the extent to which audit criteria are fulfilled. According to ISO/IEC 27000, which of the following characteristics must the audit process have?

a) It must be systematic.
b) It must be controlled by an external party.
c) It must be documented.

25) Which of the following statements are correct with respect to confidentiality and integrity of information?

a) An appropriate level of confidentiality and integrity can only be achieved by the use of encryption and digital signatures.
b) Confidentiality is the result of protecting information against their disclosure to unauthorized persons.
c) Information that are not confidential can not be protected in their integrity.

26) For which topics does ISO/IEC 27001 (Annex A) define control objectives and controls in the context of section "Operations security" (A.12)?

a) Information classification
b) Protection from malware
c) Logging and monitoring

27) For which of the following topics does ISO/IEC 27001 define control objectives and controls in Annex A?

a) Energy efficiency
b) Organization of information security
c) Compliance

28) Which properties of information should be maintained in the context of information security?

a) Integrity
b) Confidentiality
c) Invulnerability

29) What is correct with respect to processes in the context of the ISO/IEC 27000 family of standards?

a) According to ISO/IEC 27000, a process is a set of interrelated activities that transform inputs to outputs.
b) ISO/IEC 27002 defines 14 information security processes to ensure that the objectives from Annex A of ISO/IEC 27001 can be achieved.
c) Processes are part of a management system.

30) Which of the following statements are correct with respect to internal audits and management reviews?

a) A management review is carried out by the organization's top management.
b) Internal audits are carried out by an the organization's top management.
c) Management reviews must be carried out at planned intervals.