Question sheet

Name: _____

ID number: _____

Signature: _____

In order to receive the ISMS 27001 Professional 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: 75 minutes

Format: 50 multiple-choice questions, with two to six response possibilities of which one, several or all answers can be correct

Minimum points: 33 of 50

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) Which statements are correct regarding the ISO/IEC 27000 family of ISMS standards?

a) ISO/IEC 27000 describes the basics of information security management systems and defines related terms.
b) ISO/IEC 27003 contains requirements for the implementation of information security controls.
c) The full implementation of ISO/IEC 27002 is a mandatory requirement for a certification according to ISO/IEC 27001.
d) ISO/IEC 27001 contains requirements for an ISMS.

2) In the context of physical and environmental security, which of the following controls are related to the control objective "Equipment" (A.11.2)?

a) User access provisioning
b) Review of user access rights
c) Clear desk and clear screen policy

3) Which of the following controls are related to the control objective "compliance with legal and contractual requirements" (A.18.1)?

a) Compliance with physical laws
b) Protection of records in accordance with legislatory, regulatory, contractual and business requirements.
c) Privacy and protection of personally identifiable information

4) What needs to be determined by an organization according to ISO/IEC 27001 (among other things) for internal and external communication in the context of the ISMS?

a) Thresholds and limits of communication costs
b) With whom to communicate
c) Which communication is to be classified as undesirable
d) What to communicate

5) According to ISO/IEC 27001, which of the following requirements must the information security policy fulfil?

a) It must be appropriate for the purpose of the organization.
b) It must be communicated within the organization.
c) It must contain information security objectives.
d) It must include a commitment to continual improvement.

6) Which of the following policies, procedures and measures are related to the reference controls in the areas of "Operations security" (A.12) or "System acquisition, development and maintenance (A.14)?

a) Provision of user access rights
b) Controls against malware
c) Protection of transactions in application services
d) Separation of development, test and operating environments

7) Which of the following statements are correct with respect to information security risk management and its sub-processes according to ISO/IEC 27000 and ISO/IEC 27001?

a) Risk analysis is part of the risk assessment
b) As part of the risk assessment, the risk level is determined.
c) During risk assessment, the results of the risk analysis are the basis for risk evaluation.
d) Risk evaluation is part of the risk assessment

8) For which topics does ISO/IEC 27001 define requirements in section "Support" (7)?

a) Resources
b) 24 hours support
c) Communication

9) What needs to be determined by an organization according to ISO/IEC 27001 (among other things) for internal and external communication in the context of the ISMS?

a) With whom to communicate
b) Which communication is to be classified as undesirable
c) What to expect as the return on investment (ROI) from communication with external stakeholders

10) Which of the following policies, procedures and measures are related to the reference controls in the areas of "Operations security" (A.12) or "System acquisition, development and maintenance (A.14)?

a) Provision of user access rights
b) System change control procedures
c) Change management

11) You are reviewing the physical and environmental security controls (A.11) implemented in your organization for conformity against ISO/IEC 27001. According to the statement of applicability, no exclusions have been made. Which of the following circumstances constitute a deviation or a nonconformity?

a) There are several delivery and loading areas on the organization's premises.
b) Defective laptop computers, for which a repair seems uneconomical, are disposed of at the recycling center. Procedures for secure disposal do not exist.
c) There is no electronic locking system. All doors are only secured with mechanical locks.

12) Which of the following controls are (among others) related to the objective of identifying organizational assets and defining appropriate protection responsibilities (A.8.1) according to ISO/IEC 27001 (Annex A)?

a) Secure login procedures
b) Ownership of assets
c) Acceptable use of assets

13) What are the requirements of ISO/IEC 27001 with regard to internal audits?

a) The organization shall audit its customers.
b) The organization shall establish an audit program.
c) The organization shall perform at least as many internal audits as external audits are conducted.

14) Which of the following rules on the management of removable media can help prevent unauthorized disclosure of information stored on these media?

a) Information classified as confidential must be encrypted when storing them on removable media.
b) When storing data on removable media for a longer period of time, care must be taken to ensure that the temperature and humidity in the room is adequate.
c) Backup copies of information stored on removable media are taken regularly.

15) Which of the following statements are correct with respect to information security risk management and its sub-processes according to ISO/IEC 27000 and ISO/IEC 27001?

a) Risk assessment is part of the risk treatment
b) Risk identification is part of the risk assessment
c) As part of the risk assessment, the risk level is determined.

16) As part of an ISMS project aiming at achieving conformity against ISO/IEC 27001, you are investigating which regulations your organization has implemented with regard to the selection and employment of new personnel. Which of the following regulations or situations represent a nonconformity that needs to be corrected?

a) Security screening of applicants takes place, but to varying extent and in varying thoroughness, which depends on the position for which a candidate for employment is evaluated.
b) Information security responsibilities are defined as part of the contractual arrangements with employees. However, they are not explicitly stated in the contract. Instead, only a reference is made to the obligation to comply with relevant policies.
c) Screening takes place for selected applicants. Whether or not and to which extent screening is happening depends on the individual decision of the responsible staff member in the HR department.
d) Background verification checks of candidates for employment do not include a review of social media profiles.

17) According to ISO/IEC 27001, which of the following requirements must the information security policy fulfil?

a) It must contain information security objectives.
b) It must be approved by all employees.
c) It must be appropriate for the purpose of the organization.

18) Which of the following statements are correct in the context of information security aspects of business continuity management (A.17)?

a) The maintenance of an adequate level of information security in crisis and disaster situations must be planned.
b) Information security continuity controls need to be verified at regular intervals in order to ensure that they are valid and effective during adverse situations.
c) For supporting utilities, ISO/IEC 27001 requires the realization of an "n+1" redundancy.

19) Which statements about information security incidents are true?

a) All identified information security incidents must be responded to.
b) An accumulation of several information security events has to be defined as an information security problem.
c) An information security incident may occur, if a vulnerability is exploited by a threat.

20) In an organization, the controls related to communication security (A.13) are to be audited in a few months. What circumstances would be considered a nonconformity and should therefore be improved before the audit?

a) There are no precautions for securing application services in public networks.
b) The separation of networks takes place only via virtual private networks (VPN).
c) There is no policy for information transfer.
d) Not all traffic over the communication networks is encrypted.

21) Which statements are correct regarding the ISO/IEC 27000 family of ISMS standards?

a) The full implementation of ISO/IEC 27002 is a mandatory requirement for a certification according to ISO/IEC 27001.
b) ISO/IEC 27000, ISO/IEC 27004 and ISO/IEC 27008 specify requirements.
c) ISO/IEC 27002 includes guidance for the implementation of information security controls.

22) Your organization plans to outsource the business data warehousing. The company ACME IT applies for this contract. ACME IT advertises that they are "certified against ISO/IEC 27001". You know that the certificate is up-to-date and valid, but you do not have any further information. What does the existence of the certificate imply, and which of the following statements are correct in this context?

a) All IT services provided by ACME IT are governed by the ISMS.
b) An accredited certification body has confirmed that the ISMS of ACME IT complies with the requirements of ISO/IEC 27001.
c) ACME IT operates an ISMS.

23) Your mission is to help an organization achieve the control objective "To ensure the security of teleworking and use of mobile devices" (A.6.2). The organization allows both the use of mobile devices as well as teleworking. Both are largely unregulated, especially with regard to information security. What do you need to implement or ensure in order to achieve conformity with ISO/IEC 27001?

a) Establish a mobile device policy
b) Treatment of risks associated with the use of laptop computers
c) Ensure that there are identical rules for teleworking and remote working during business trips
d) Assessment of risks associated with mobile device usage and teleworking

24) As part of an ISMS project aiming at achieving conformity against ISO/IEC 27001, you are investigating which regulations your organization has implemented with regard to the selection and employment of new personnel. Which of the following regulations or situations represent a nonconformity that needs to be corrected?

a) Screening takes place for selected applicants. Whether or not and to which extent screening is happening depends on the individual decision of the responsible staff member in the HR department.
b) Security screening of applicants takes place, but violates a recently enacted law on protecting privacy.
c) Background verification checks of candidates for employment do not take into account the creditworthiness of the candidates (i.e. no information from a credit protection agency is obtained).

25) Which of the following reflect the control objectives in the area of "operations security" (A.12) according to ISO/IEC 27001?

a) To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
b) To ensure the protection of data used for testing.
c) To ensure that auditing activities during operation are effectively prevented.
d) To ensure that information and information processing facilities are protected against malware.

26) What are the requirements of ISO/IEC 27001 with regard to internal audits?

a) The organization shall conduct an internal audit at least every 6 months.
b) The organization shall audit its customers.
c) The organization shall establish an audit program.
d) The organization shall define the audit criteria for each audit.

27) Which of the following controls are (among others) related to the objective of identifying organizational assets and defining appropriate protection responsibilities (A.8.1) according to ISO/IEC 27001 (Annex A)?

a) Ownership of assets
b) Physical access control
c) Secure login procedures
d) Acceptable use of assets

28) According to ISO/IEC 27001 (section 8), what are requirements for the operation of an ISMS?

a) The organization shall implement plans to achieve information security objectives determined.
b) The organization shall plan, implement and control the processes needed to meet information security requirements.
c) The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

29) Cryptographic controls can help to achieve various information security goals. Which of the following goals can be supported by using encryption and digital signatures?

a) Integrity
b) Authenticity
c) Reliability

30) Cryptographic controls can help to achieve various information security goals. Which of the following goals can be supported by using encryption and digital signatures?

a) Integrity
b) Confidentiality
c) Authenticity
d) Reliability

31) According to ISO/IEC 27001 (section 8), what are requirements for the operation of an ISMS?

a) The organization shall ensure that outsourced processes are determined and controlled.
b) The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.
c) The organization shall retain documented information of the results of the information security risk assessments.
d) The organization shall plan, implement and control the processes needed to meet information security requirements.

32) Which of the following basic principles contribute to the successful implementation of an ISMS according to ISO/IEC 27000?

a) Backend security comes before client security
b) Awareness of the need for information security
c) Security through obscurity

33) You are reviewing the physical and environmental security controls (A.11) implemented in your organization for conformity against ISO/IEC 27001. According to the statement of applicability, no exclusions have been made. Which of the following circumstances constitute a deviation or a nonconformity?

a) There is no electronic locking system. All doors are only secured with mechanical locks.
b) It is common for administrators and other employees to take home their computers over the weekend without any kind of approval. Since all devices have been returned in the past, this is tolerated by the organization's management.
c) No preventive measures have been implemented against the effects of earthquakes.
d) There are several delivery and loading areas on the organization's premises.

34) According to ISO/IEC 27001, what is part of the evaluation of information security risks or needs to be considered when planning this activity?

a) Defining security acceptance criteria for new services and applications
b) Defining criteria for conducting information security risk assessments
c) Estimation of the realistic probability of occurrence of the identified risks

35) Which of the following statements are correct in the context of information security aspects of business continuity management (A.17)?

a) Information security continuity controls need to be verified at regular intervals in order to ensure that they are valid and effective during adverse situations.
b) The maintenance of an adequate level of information security in crisis and disaster situations must be planned.
c) Information processing facilities shall be implemented with redundancy to meet availability requirements.
d) Information security considerations in business continuity management may be excluded from the applicability to the ISMS without further justification in the statement of applicability.

36) Which of the following controls are (among others) related to the objective of a consistent and effective approach to the management of information security incidents (A.16.1) according to ISO/IEC 27001 (Annex A)?

a) Collection of evidence
b) Controls against malware
c) Segregation of duties

37) Which statements about information security incidents are true?

a) Every information security incident is a single or a series of information security events.
b) An accumulation of several information security events has to be defined as an information security problem.
c) An information security incident may be produced by an attacker.
d) Every information security event results into an information security incident.

38) What is correct in the context of ISMS certification according to ISO/IEC 27001 (in Europe)?

a) Evidence of attending a certified training must be provided by the responsible information security officer as a prerequisite for the certification of the ISMS against ISO/IEC 27001.
b) The certification body must comply with the requirements of ISO/IEC 27006.
c) As part of the certification, a certification audit is conducted on behalf of the certification body to verify the conformity of the ISMS with the requirements of the ISO/IEC 27001 standard.

39) Which of the following controls are related to the control objective "operational procedures and responsibilities" (A.12.1)?

a) Change management
b) Documented operating procedures
c) Capacity management
d) Clock synchronization

40) Your mission is to help an organization achieve the control objective "To ensure the security of teleworking and use of mobile devices" (A.6.2). The organization allows both the use of mobile devices as well as teleworking. Both are largely unregulated, especially with regard to information security. What do you need to implement or ensure in order to achieve conformity with ISO/IEC 27001?

a) Ensure that there are identical rules for teleworking and remote working during business trips
b) Establish a policy and supporting security measures for teleworking
c) Treatment of risks associated with the use of laptop computers

41) According to ISO/IEC 27001, what must be subject to human resource security during employment?

a) The disciplinary process is confidential and only communicated to senior staff members.
b) Appropriate education, training and related actions promote awareness among all employees on information security.
c) The personnel records of all employees have been reviewed and approved by the information security officer.
d) Management requires all employees and contractors to apply information security in accordance with the established policies.

42) Which of the following basic principles contribute to the successful implementation of an ISMS according to ISO/IEC 27000?

a) Ensuring non-verifiability of compliance violations
b) Backend security comes before client security
c) Redundant allocation of responsibilities for information security
d) Ensuring a comprehensive approach to information security management

43) For which topics does ISO/IEC 27001 define requirements in section "Support" (7)?

a) Documented information
b) Service desk
c) Risk support
d) 24 hours support

44) According to ISO/IEC 27001, what must be subject to human resource security during employment?

a) Appropriate education, training and related actions promote awareness among all employees on information security.
b) Management requires all employees and contractors to apply information security in accordance with the established policies.
c) The personnel records of all employees have been reviewed and approved by the information security officer.

45) Which of the following controls are (among others) related to the objective of a consistent and effective approach to the management of information security incidents (A.16.1) according to ISO/IEC 27001 (Annex A)?

a) Reporting information security events
b) Collection of evidence
c) Controls against malware
d) Response to information security incidents

46) In the context of physical and environmental security, which of the following controls are related to the control objective "Equipment" (A.11.2)?

a) Clear desk and clear screen policy
b) Unattended user equipment
c) Removal of assets
d) User access provisioning

47) Which of the following controls are related to the control objective "operational procedures and responsibilities" (A.12.1)?

a) Documented operating procedures
b) Information security in supplier relationships
c) Secure development policy

48) According to ISO/IEC 27001, what is part of the evaluation of information security risks or needs to be considered when planning this activity?

a) Estimation of the realistic probability of occurrence of the identified risks
b) Ensuring that repeated information security risk assessments produce consistent, valid, and comparable results
c) Estimation of the possible consequences if the identified risks occur
d) Defining criteria for conducting information security risk assessments

49) Which of the following reflect the control objectives in the area of "operations security" (A.12) according to ISO/IEC 27001?

a) To prevent exploitation of technical vulnerabilities.
b) To ensure the protection of data used for testing.
c) To record events (on user activities, exceptions, faults, ...) and generate evidence.

50) Which of the following rules on the management of removable media can help prevent unauthorized disclosure of information stored on these media?

a) Files shall be deleted from removable media when they are not needed anymore.
b) Information classified as confidential must be encrypted when storing them on removable media.
c) The use of removable media is only allowed if there is a valid business purpose to do so.
d) Removable media potentially containing confidential data must be disposed of securely when no longer required, using formal procedures (e.g. multiple overwriting prior to disposal, physical destruction).