



**Free Questions for ISO-IEC-27001-Lead-Auditor by  
braindumpscollection**

**Shared by Banks on 29-01-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

**Question Type:** MultipleChoice

---

Which three of the following options are an advantage of using a sampling plan for the audit?

## Options:

---

- A- Overrides the auditor's instincts
- B- Use of the plan for consecutive audits
- C- Provides a suitable understanding of the ISMS
- D- Implements the audit plan efficiently
- E- Gives confidence in the audit results
- F- Misses key issues

## Answer:

---

C, D, E

## Explanation:

---

According to ISO 19011:2018, which provides guidelines for auditing management systems, a sampling plan is a method for selecting a representative subset of the audit evidence from a defined population<sup>1</sup>. A sampling plan can have several advantages for the audit, such as providing a suitable understanding of the ISMS by covering its key processes, activities, and controls; implementing the audit plan efficiently by optimizing the use of time and resources; and giving confidence in the audit results by ensuring that the sample is sufficient, reliable, and unbiased<sup>1</sup>. Therefore, these three options are examples of advantages of using a sampling plan for the audit. The other options are not advantages, but rather disadvantages or risks of using a sampling plan. For example, overruling the auditor's instincts may lead to missing important evidence or issues that are not covered by the sampling plan; using the same plan for consecutive audits may reduce the effectiveness and validity of the audit results; and missing key issues may result from an inadequate or inappropriate sampling plan<sup>1</sup>. Reference: ISO 19011:2018 - Guidelines for auditing management systems

## Question 2

---

**Question Type:** MultipleChoice

---

Which three of the following work documents are not required for audit planning by an auditor conducting a certification audit?

**Options:**

---

**A-** An audit plan

- B-** A sample plan
- C-** An organisation's financial statement
- D-** A checklist
- E-** A career history of the IT manager
- F-** A list of external providers

**Answer:**

---

C, E, F

**Explanation:**

---

According to ISO 19011:2018, which provides guidelines for auditing management systems, an auditor conducting a certification audit should prepare for an audit by reviewing relevant information about the auditee's context and processes<sup>1</sup>. This may include reviewing documented information related to the audited management system (such as policies, procedures, manuals), previous audit reports and records (such as findings, nonconformities, corrective actions), relevant legal and regulatory requirements (such as laws, standards), relevant risks and opportunities (such as internal and external issues), relevant performance indicators (such as objectives, targets), etc<sup>1</sup>. Therefore, an auditor may need work documents such as an audit plan (which defines what will be done during an audit), a sample plan (which defines how many samples will be taken from a population), and a checklist (which helps to ensure that all relevant aspects are covered during an audit)<sup>1</sup>. However, an auditor does not need work documents such as an organisation's financial statement (which is not directly related to information security management), a career history of the IT manager (which is not relevant to assessing conformity with ISO/IEC 27001:2022), or a list of external providers (which is not necessary for planning an audit)<sup>1</sup>. Reference: ISO 19011:2018 - Guidelines for auditing management systems

## Question 3

---

**Question Type:** MultipleChoice

---

Which six of the following actions are the individual(s) managing the audit programme responsible for?

### Options:

---

- A- Selecting the audit team
- B- Retaining documented information of the audit results
- C- Defining the objectives, scope and criteria for an individual audit
- D- Defining the plan of an individual audit
- E- Establishing the extent of the audit programme
- F- Establishing the audit programme
- G- Determining the resources necessary for the audit programme
- H- Communicating with the auditee during the audit

### Answer:

---

A, B, C, D, E, F

### **Explanation:**

---

According to ISO 19011:2018, which provides guidelines for auditing management systems, an audit programme is a set of one or more audits planned for a specific time frame and directed towards a specific purpose<sup>1</sup>. The individual(s) managing the audit programme are responsible for establishing, implementing and maintaining the audit programme in accordance with the organization's policies and objectives<sup>1</sup>. This includes defining the extent of the audit programme based on strategic direction, risks and opportunities; establishing the audit programme by defining its objectives, scope and criteria; determining the resources necessary for the audit programme; selecting competent auditors and assigning them to appropriate audits; defining the objectives, scope and criteria for each individual audit; defining the plan of each individual audit; retaining documented information of the audit results; reviewing and improving the performance of the audit programme<sup>1</sup>. Therefore, these six actions are part of the responsibilities of the individual(s) managing the audit programme. The other option, communicating with the auditee during the audit, is not a responsibility of the individual(s) managing the audit programme, but rather a responsibility of the audit team leader<sup>1</sup>. Reference: ISO 19011:2018 - Guidelines for auditing management systems

## **Question 4**

---

**Question Type: MultipleChoice**

---

Which three of the following phrases are objectives' in relation to an audit?

### Options:

---

- A- International Standard
- B- Identify opportunities for improvement
- C- Confirm the scope of the management system
- D- Management policy
- E- Complete audit on time
- F- Regulatory requirements

### Answer:

---

B, C, F

### Explanation:

---

According to ISO 19011:2018, which provides guidelines for auditing management systems, the audit objectives are defined by the audit client and may include determining the extent of conformity or nonconformity of the audited management system against the audit criteria, evaluating the ability of the audited management system to ensure that the organization meets applicable statutory, regulatory and contractual requirements, identifying potential improvement opportunities for the audited management system, and facilitating continual improvement of the audited management system<sup>1</sup>. Therefore, these three phrases are examples of objectives in relation to an audit. The other options are not objectives, but rather elements or factors that may influence or affect an audit. For example, an international standard is a source of audit criteria, a management policy is a part of the audited management system, and completing an audit on time is a requirement for an effective audit. Reference: ISO 19011:2018 - Guidelines for auditing management systems

## Question 5

---

**Question Type:** DragDrop

---

Select the words that best complete the sentence:

To complete the sentence with the best word(s), click on the blank section you want to complete so that it is highlighted in red, and then click on the applicable text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

It is the sole responsibility of a third-party audit team leader to

**Answer:**

---

## Question 6

**Question Type:** MultipleChoice

---

Identify non-conformances in the management system

Be half of the certification body

Compile checklists for the audit team

Identify non-conformances

In the context of a third-party certification audit, confidentiality is an issue in an audit programme. Select two options which correctly state the function of confidentiality in an audit



### Options:

---

- A- Auditors are forced by regulatory requirements to maintain confidentiality in an audit
- B- Observers in an audit team cannot access any confidential information
- C- Confidentiality is one of the principles of audit conduct
- D- Auditors should obtain the auditee's permission before using a camera or recording equipment
- E- Audit information can be used for improving personal competence by the auditor
- F- As an auditor is always accompanied by a guide, there is no risk to the auditee's sensitive information

### Answer:

---

C, D

### Explanation:

---

Confidentiality is one of the principles of audit conduct that auditors should adhere to when performing audits. Confidentiality means that auditors should exercise discretion in the use and protection of information acquired in the course of their duties<sup>3</sup>. Auditors should respect the intellectual property rights of the auditee and other parties involved in the audit, and should not disclose any information that is sensitive, proprietary, or confidential without prior approval from the auditee or other authorized parties<sup>3</sup>. Auditors should also obtain the auditee's permission before using a camera or recording equipment during an audit, as these devices may capture confidential information or infringe on the privacy of individuals<sup>3</sup>. Therefore, these two options correctly state the function of confidentiality in an audit. The other options are either incorrect or irrelevant to confidentiality. For example, auditors are not forced by regulatory requirements to maintain confidentiality in an audit, but rather by ethical obligations and contractual agreements<sup>3</sup>. Observers in an audit

team can access confidential information if they have signed a confidentiality agreement and have been authorized by the auditee<sup>3</sup>. Audit information can be used for improving personal competence by the auditor only if it does not compromise confidentiality or conflict with other interests<sup>3</sup>. As an auditor is always accompanied by a guide, there is still a risk to the auditee's sensitive information if the guide is not trustworthy or authorized to access such information<sup>3</sup>. Reference: ISO 19011:2018 - Guidelines for auditing management systems

## Question 7

---

**Question Type:** MultipleChoice

---

Which two of the following are examples of audit methods that 'do' involve human interaction?

### **Options:**

---

- A-** Performing an independent review of procedures in preparation for an audit
- B-** Reviewing the auditee's response to an audit finding
- C-** Analysing data by remotely accessing the auditee's server
- D-** Observing work performed by remote surveillance
- E-** Analysing data by remotely accessing the auditee's server

**Answer:**

---

A, B

**Explanation:**

---

Audit methods are techniques used by auditors to obtain audit evidence. Audit methods can be classified into two categories: those that involve human interaction and those that do not<sup>2</sup>. Audit methods that involve human interaction require direct communication between the auditor and the auditee or other relevant parties, such as interviews, questionnaires, surveys, meetings, etc. Audit methods that do not involve human interaction rely on observation, inspection, measurement, testing, sampling, analysis, etc., without requiring any verbal or written exchange<sup>2</sup>. Therefore, performing an independent review of procedures in preparation for an audit and reviewing the auditee's response to an audit finding are examples of audit methods that involve human interaction, as they require reading and evaluating documents provided by the auditee or other sources. On the other hand, analysing data by remotely accessing the auditee's server and observing work performed by remote surveillance are examples of audit methods that do not involve human interaction, as they do not require any direct communication with the auditee or other parties. Reference: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) | CQI | IRCA

## Question 8

---

**Question Type:** DragDrop

---

Please match the roles to the following descriptions:

1. The organisation or person requesting an audit

2. The organisation as a whole or parts thereof being audited

**Answer:** A person who provides specific knowledge or expertise relating to the organisation, activity, process, product, service or discipline to be audited

**Explanation:** A person who accompanies the audit team but does not act as an auditor

[ISO 19011:2022 Guidelines for auditing management systems]

[ISO/IEC 17021-1:2022 Conformity assessment --- Requirements for bodies providing audit and certification of management systems --- Part 1: Requirements]

A horizontal bar containing seven role labels: Auditor, Auditor leader, Audit client, Observer, Auditee, Technical expert, and Auditor.

## Question 9

**Question Type:** MultipleChoice

Which two activities align with the "Check" stage of the Plan-Do-Check-Act cycle when applied to the process of managing an internal audit program as described in ISO 19011?

### Options:

---

- A- Retains records of internal audits
- B- Define audit criteria and scope for each internal audit
- C- Update the internal audit programme
- D- Establish a risk-based internal audit programme
- E- Conduct internal audits
- F- Verify effectiveness of the internal audit programme
- G- Review trends in internal audit result

### Answer:

---

F, G

### Explanation:

---

The Check stage of the PDCA cycle involves monitoring and measuring the performance of the process and comparing it with the planned objectives and criteria. In the context of managing an internal audit programme, this stage includes verifying the effectiveness of the internal audit programme by evaluating whether it meets its objectives, scope, and criteria, and whether it is implemented in accordance with ISO 19011 guidelines<sup>1</sup>. It also includes reviewing the trends in internal audit results by analyzing the data collected from the audits, such as audit findings, nonconformities, corrective actions, opportunities for improvement, and customer

## Question 10

---

**Question Type:** DragDrop

---

Select a word from the following options that best completes the sentence:

To complete the sentence with the word(s) click on the blank section you want to complete so that it is highlighted in red, and then click on the application text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

"The purpose of a management system audit is to  the performance of an organisation's management system"

**Answer:**

research

manage

evaluate

research

## Question 11

---

**Question Type:** DragDrop

---

Select the words that best complete the sentence:

To complete the sentence with the word(s) click on the blank section you want to complete so that it is highlighted in red, and then click on the application text from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

\*An accredited certification assures the

of the

**Answer:**

---

reliability

the certification body

report

clarity

competence of the audit team

decision made by the certification body

reliability

**To Get Premium Files for ISO-IEC-27001-Lead-Auditor Visit**

**<https://www.p2pexams.com/products/iso-iec-27001-lead-auditor>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/pcb/pdf/iso-iec-27001-lead-auditor>**

