
# Free Questions for ISO-IEC-27001-Lead-Auditor by certsdeals

## Shared by Conner on 12-12-2023

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including misaddressed labels and, in 15% of cases, two or more labels for different addresses for the one package. You are interviewing the Shipping Manager (SM).

You: Are items checked before being dispatched?

SM: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.

You: What action is taken when items are returned?

SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.

You raise a nonconformity against ISO 27001:2022 based on the lack of control of the labelling process.

At the closing meeting, the Shipping Manager issues an apology to you that his comments may have been misunderstood. He says that he did not realise that there is a background IT process that automatically checks that the right label goes onto the right parcel otherwise the parcel is ejected at labelling. He asks that you withdraw your nonconformity.

Select three options of the correct responses that you as the audit team leader would make to the request of the Shipping Manager.

## Options:

**A-** Advise the Shipping Manager that his request will be included in the audit report

**B-** Advise management that the new information provided will be discussed when the auditors have more time

**C-** Inform the Shipping Manager that the nonconformity is minor and should be quickly corrected

**D-** Ask the audit team members to state what they think should happen

**E-** Inform him of your understanding and withdraw the nonconformity

**F-** Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed

**G-** Advise the Shipping Manager that the nonconformity must stand since the evidence obtained for it was dear

**H-** Indicate that the nonconformity is evidence of a deeper system failure that needs to be rectified

## Answer:

A, B, F

## Explanation:

A) Advise the Shipping Manager that his request will be included in the audit report. This is true because the audit report should document all the relevant information and evidence related to the audit, including any requests or objections raised by the auditee.The audit report should also provide the rationale for the audit conclusions and recommendations12.

B) Advise management that the new information provided will be discussed when the auditors have more time. This is true because the auditors should not make hasty decisions based on incomplete or unverified information.The auditors should review and evaluate the new information in a systematic and objective manner, and determine whether it affects the audit findings, nonconformities, or conclusions12.

F) Thank the Shipping Manager for his honesty but advise that withdrawing the nonconformity is not the right way to proceed. This is true because the auditors should acknowledge and appreciate the cooperation and transparency of the auditee, but also maintain their professional integrity and independence.The auditors should not withdraw a nonconformity unless they are satisfied that it was raised in error or that it has been effectively corrected and verified12.

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

# Question 2

**Question Type:** **MultipleChoice**

You are conducting an ISMS audit in the despatch department of an international logistics organisation that provides shipping services to large organisations including local hospitals and government offices. Parcels typically contain pharmaceutical products, biological samples, and documents such as passports and driving licences. You note that the company records show a very large number of returned items with causes including mis-addressed labels and, in 15% of company cases, two or more labels for different addresses for

the one package. You are interviewing the Shipping Manager (SM).

You: Are items checked before being dispatched?

SH: Any obviously damaged items are removed by the duty staff before being dispatched, but the small profit margin makes it uneconomic to implement a formal checking process.

You: What action is taken when items are returned?

SM: Most of these contracts are relatively low value, therefore it has been decided that it is easier and more convenient to simply reprint the label and re-send individual parcels than it is to implement an investigation.

You raise a nonconformity. Referencing the scenario, which six of the following Appendix A controls would you expect the auditee to have implemented when you conduct the follow-up audit?

## Options:

**A-** 5.11 Return of assets

**B-** 8.12 Data leakage protection

**C-** 5.3 Segregation of duties

**D-** 6.3 Information security awareness, education, and training

**E-** 7.10 Storage media

**F-** 8.3 Information access restriction

**G-** 5.6 Contact with special interest groups

**H-** 6.4 Disciplinary process

**I-** 7.4 Physical security monitoring

**J-** 5.13 Labelling of information

**K-** 5.32 Intellectual property rights

## Answer:

B, D, E, F, I, J

## Explanation:

B) 8.12 Data leakage protection. This is true because the auditee should have implemented measures to prevent unauthorized disclosure of sensitive information, such as personal data, medical records, or official documents, that are contained in the parcels.Data leakage protection could include encryption, authentication, access control, logging, and monitoring of data transfers12.

D) 6.3 Information security awareness, education, and training. This is true because the auditee should have ensured that all employees and contractors involved in the shipping process are aware of the information security policies and procedures, and have received appropriate training on how to handle and protect the information assets in their custody.Information security awareness, education, and training could include induction programmes, periodic refreshers, awareness campaigns, e-learning modules, and feedback mechanisms13.

E) 7.10 Storage media. This is true because the auditee should have implemented controls to protect the storage media that contain information assets from unauthorized access, misuse, theft, loss, or damage.Storage media could include paper documents, optical

disks, magnetic tapes, flash drives, or hard disks14.Storage media controls could include physical locks, encryption, backup, disposal, or destruction14.

F) 8.3 Information access restriction. This is true because the auditee should have implemented controls to restrict access to information assets based on the principle of least privilege and the need-to-know basis.Information access restriction could include identification, authentication, authorization, accountability, and auditability of users and systems that access information assets15.

I) 7.4 Physical security monitoring. This is true because the auditee should have implemented controls to monitor the physical security of the premises where information assets are stored or processed.Physical security monitoring could include CCTV cameras, alarms, sensors, guards, or patrols16.Physical security monitoring could help detect and deter unauthorized physical access or intrusion attempts16.

J) 5.13 Labelling of information. This is true because the auditee should have implemented controls to label information assets according to their classification level and handling instructions.Labelling of information could include markings, tags, stamps, stickers, or barcodes1.Labelling of information could help identify and protect information assets from unauthorized disclosure or misuse1.

ISO/IEC 27002:2022 Information technology --- Security techniques --- Code of practice for information security controls

ISO/IEC 27001:2022 Information technology --- Security techniques --- Information security management systems --- Requirements

ISO/IEC 27003:2022 Information technology --- Security techniques --- Information security management systems --- Guidance

ISO/IEC 27004:2022 Information technology --- Security techniques --- Information security management systems --- Monitoring measurement analysis and evaluation

ISO/IEC 27005:2022 Information technology --- Security techniques --- Information security risk management

ISO/IEC 27006:2022 Information technology --- Security techniques --- Requirements for bodies providing audit and certification of information security management systems

[ISO/IEC 27007:2022 Information technology --- Security techniques --- Guidelines for information security management systems auditing]

# Question 3

**Question Type:** MultipleChoice

You are an experienced ISMS audit team leader guiding an auditor in training. You are testing her understanding of follow-up audits by asking her a series of questions to which the answer is either "true* or 'false'. Which four of the following questions should the answer be true"'

## Options:

**A-** A follow-up audit may be carried out where nonconformities are major

**B-** A follow-up audit may be carried out where nonconformities are minor

**C-** The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified

**D-** The outcome of a follow-up audit could lower a major nonconformity to minor status

**E-** The outcome of a follow-up audit could be a recommendabon to suspend the client's certification

**F-** The outcomes of a follow-up audit should be reported to the individual managing the audit programme and the audit client

**G-** A follow-up audit is required in all instances where nonconformities have been identified

**H-** A follow-up audit is required only in instances where a major nonconformity has been identified

## Answer:

A, B, C, F

## Explanation:

A follow-up audit may be carried out where nonconformities are major. This is true because a major nonconformity is a situation that raises significant doubt about the ability of the organization's management system to achieve its intended results, and therefore requires immediate corrective action.A follow-up audit is necessary to verify the effectiveness of the corrective action and the conformity of the management system12.

A follow-up audit may be carried out where nonconformities are minor. This is true because a minor nonconformity is a situation that does not affect the capability of the management system to achieve its intended results, but represents a deviation from the specified requirements.A follow-up audit may be conducted to check the implementation of the corrective action and the improvement of the management system12.

The outcomes of a follow-up audit should be reported to top management and the audit team leader who carried out the audit where the nonconformities were initially identified. This is true because the top management is responsible for ensuring the effectiveness and

continual improvement of the management system, and the audit team leader is accountable for the audit process and the audit conclusions.The follow-up audit report should provide them with objective evidence of the status of the nonconformities and the corrective actions taken by the auditee13.

The outcomes of a follow-up audit should be reported to the individual managing the audit programme and the audit client. This is true because the individual managing the audit programme is responsible for planning, implementing, monitoring and reviewing the audit activities, and the audit client is the organization or person requesting an audit.The follow-up audit report should inform them of the results of the follow-up audit and any changes in the certification status of the auditee13.

ISO 19011:2022 Guidelines for auditing management systems

ISO/IEC 27001:2022 Information technology --- Security techniques --- Information security management systems --- Requirements

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

# Question 4

**Question Type:** **MultipleChoice**

You are an experienced ISMS audit team leader guiding an auditor in training. Your team has just completed a third-party surveillance audit of a mobile telecom provider. The auditor in training asks you how you intend to prepare for the Closing meeting. Which four of the following are appropriate responses?

## Options:

**A-** I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these

**B-** I will instruct my audit team to wait outside the auditee's offices so we can leave as quickly as possible after the closing meeting. This saves our time and the client's time too

**C-** It is not necessary to prepare for the closing meeting. Once you have carried out as many audits as I have you already know what needs to be discussed

**D-** I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented

**E-** I will contact head office to ensure our invoice has been paid, If not, I will cancel the closing meeting and temporarily withhold the audit report

**F-** I will discuss any follow-up required with my audit team

**G-** I will review and, as appropriate, approve my teams audit conclusions

**H-** I will review the audit evidence and the audit findings with the rest of the team

## Answer:

A, D, F, H

## Explanation:

According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.6 requires the audit team leader to conduct a closing meeting with the auditee's representatives at the end of the audit to present the audit conclusions and any findings1.The closing meeting should also provide an opportunity for the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1. Therefore, when preparing for the closing meeting, an ISMS auditor should consider the following actions:

I will advise the auditee that the purpose of the closing meeting is for the audit team to communicate our findings. It is not an opportunity for the auditee to challenge these: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to collecting and evaluating audit evidence and reaching audit conclusions. The auditor should advise the auditee that the purpose of the closing meeting is for the audit team to communicate their findings, which are based on objective evidence and professional judgement. The auditor should also explain that it is not an opportunity for the auditee to challenge these findings, as they have already been discussed and confirmed during the audit.However, the auditor should also invite the auditee to ask questions, clarify issues, acknowledge the findings, and comment on the audit process1.

I will schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented: This action is appropriate because it reflects the fact that the auditor has followed a planned and agreed audit programme and schedule.The auditor should schedule a closing meeting with the auditee's representatives at which the audit conclusions will be presented, in accordance with clause 6.6 of ISO 19011:20181.The auditor should also ensure that the closing meeting is attended by those responsible for managing or implementing the ISMS, as well as any other relevant parties1.

I will discuss any follow-up required with my audit team: This action is appropriate because it reflects the fact that the auditor has followed a risk-based approach to determining and reporting any follow-up actions required by the auditee or the certification body.The auditor should discuss any follow-up required with their audit team, such as verifying corrective actions for nonconformities or conducting a subsequent audit1.The auditor should also document any follow-up actions in the audit report1.

I will review and, as appropriate, approve my teams audit conclusions: This action is appropriate because it reflects the fact that the auditor has followed a rigorous and professional process to reaching and reporting audit conclusions. The auditor should review and, as

appropriate, approve their teams audit conclusions, which are based on objective evidence and professional judgement.The auditor should also ensure that their teams audit conclusions are consistent with the audit objectives and scope, and reflect the overall performance and conformity of the ISMS1.

# Question 5

**Question Type:** MultipleChoice

You are an ISMS audit team leader tasked with conducting a follow-up audit at a client's data centre. Following two days on-site you conclude that of the original 12 minor and 1 major nonconformities that prompted the follow-up audit, only 1 minor nonconformity still remains outstanding.

Select four options for the actions you could take.

## Options:

**A-** Book another follow-up audit on-site to review the one outstanding minor nonconformity once it has been cleared

**B-** Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit

**C-** Advise the auditee that you will arrange an online audit to deal with the outstanding nonconformity

**D-** Note the progress made but hold the audit open until all corrective action has been cleared

**E-** Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified

**F-** Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity

**G-** Recommend suspension of the organisation's certification as they have failed to implement the agreed corrections and corrective actions within the agreed timescale

**H-** Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised

## Answer:

B, E, F, H

## Explanation:

According to ISO 19011:2018, which provides guidelines for auditing management systems, clause 6.7 requires the audit team leader to conduct a follow-up audit to verify the implementation and effectiveness of the corrective actions taken by the auditee in response to the nonconformities identified during a previous audit1.The follow-up audit should be conducted in accordance with the same principles and processes as the initial audit, and should result in a conclusion on the status of the nonconformities and any remaining issues1. Therefore, when conducting a follow-up audit, an ISMS auditor should consider the following actions:

Recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit: This action is appropriate because it reflects the fact that the auditee has cleared most of the nonconformities, including the major one, and only one minor nonconformity remains outstanding.A minor nonconformity is defined as a failure to achieve one or more requirements of ISO/IEC 27001:2022 or a situation which raises significant doubt about the ability of an ISMS process to achieve its intended output, but does not affect its overall

effectiveness or conformity2. Therefore, this finding does not prevent or preclude the continuation of certification, as long as it is addressed by appropriate corrective actions within a reasonable time frame.The auditor should recommend that the outstanding minor nonconformity is dealt with at the next surveillance audit, which is a regular audit conducted by the certification body to confirm the ongoing conformity and effectiveness of an ISMS3.

Agree with the auditee/audit client how the remaining nonconformity will be cleared, by when, and how its clearance will be verified: This action is appropriate because it reflects the fact that the auditee has demonstrated commitment and capability to implement corrective actions for the nonconformities identified during the previous audit. The auditor should agree with the auditee/audit client on a realistic, achievable, and effective corrective action plan for the remaining nonconformity, including a clear deadline and verification method.The auditor should also document this agreement in the follow-up audit report1.

Advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity: This action is appropriate because it reflects the fact that the auditor has followed a systematic and consistent approach to conducting and reporting the follow-up audit. The auditor should advise the individual managing the audit programme of any decision taken regarding the outstanding nonconformity, such as recommending its closure at the next surveillance audit or agreeing on a corrective action plan with the auditee/audit client.The auditor should also provide sufficient information and evidence to support their decision1.

Close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised: This action is appropriate because it reflects the fact that the organisation has achieved satisfactory results in the follow-up audit. The auditor should close the follow-up audit as the organisation has demonstrated it is committed to clearing the nonconformities raised by implementing effective corrective actions for most of them and agreeing on a plan for the remaining one.The auditor should also communicate the follow-up audit conclusion to the auditee/audit client and other relevant parties1.

# Question 6

**Question Type:** MultipleChoice

You are performing an ISMS audit at a nursing home where residents always wear an electronic wristband for monitoring their location, heartbeat, and blood pressure. The wristband automatically uploads this data to a cloud server for healthcare monitoring and analysis by staff.

You now wish to verify that the information security policy and objectives have been established by top management. You are sampling the mobile device policy and identify a security objective of this policy is "to ensure the security of teleworking and use of mobile devices" The policy states the following controls will be applied in order to achieve this.

Personal mobile devices are prohibited from connecting to the nursing home network, processing, and storing residents'

data.

The company's mobile devices within the ISMS scope shall be registered in the asset register.

The company's mobile devices shall implement or enable physical protection, i.e., pin-code protected screen lock/unlock,

facial or fingerprint to unlock the device.

The company's mobile devices shall have a regular backup.

To verify that the mobile device policy and objectives are implemented and effective, select three options for your audit trail.

## Options:

**A-** Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home

**B-** Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home

**C-** Review the internal audit report to make sure the IT department has been audited

**D-** Review the asset register to make sure all personal mobile devices are registered

**E-** Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register

**F-** Review the asset register to make sure all company's mobile devices are registered

**G-** Interview the supplier of the devices to make sure they are aware of the ISMS policy

**H-** Interview top management to verify their involvement in establishing the information security policy and the information security objectives

## Answer:

C, E, F

## Explanation:

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 5.2 requires top management to establish an information security policy that provides the framework for setting information security objectives1.Clause 6.2 requires top management to ensure that the information security objectives are established at relevant functions and levels1. Therefore, when verifying that the information security

policy and objectives have been established by top management, an ISMS auditor should review relevant documents and records that demonstrate top management's involvement and commitment.

To verify that the mobile device policy and objectives are implemented and effective, an ISMS auditor should review relevant documents and records that demonstrate how the policy and objectives are communicated, monitored, measured, analyzed, and evaluated. The auditor should also sample and verify the implementation of the controls that are stated in the policy.

Three options for the audit trail that are relevant to verifying the mobile device policy and objectives are:

Review the internal audit report to make sure the IT department has been audited: This option is relevant because it can provide evidence of how the IT department, which is responsible for managing the mobile devices and their security, has been evaluated for its conformity and effectiveness in implementing the mobile device policy and objectives. The internal audit report can also reveal any nonconformities, corrective actions, or opportunities for improvement related to the mobile device policy and objectives.

Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register: This option is relevant because it can provide evidence of how the mobile devices that are used by the medical staff, who are involved in processing and storing residents' data, are registered in the asset register and have physical protection enabled. This can verify the implementation and effectiveness of two of the controls that are stated in the mobile device policy.

Review the asset register to make sure all company's mobile devices are registered: This option is relevant because it can provide evidence of how the company's mobile devices that are within the ISMS scope are identified and accounted for. This can verify the implementation and effectiveness of one of the controls that are stated in the mobile device policy.

The other options for the audit trail are not relevant to verifying the mobile device policy and objectives, as they are not related to the policy or objectives or their implementation or effectiveness. For example:

Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding physical security or access control, but not specifically to mobile devices.

Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security awareness or compliance, but not specifically to mobile devices.

Interview the supplier of the devices to make sure they are aware of the ISMS policy: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to another policy or objective regarding information security within supplier relationships, but not specifically to mobile devices.

Interview top management to verify their involvement in establishing the information security policy and the information security objectives: This option is not relevant because it does not provide evidence of how the mobile device policy and objectives are implemented or effective. It may be related to verifying that the information security policy and objectives have been established by top management, but not specifically to mobile devices.

# Question 7

**Question Type:** MultipleChoice

You are carrying out your first third-party ISMS surveillance audit as an Audit Team Leader. You are presently in the auditee's data centre with another member of your audit team.

Your colleague seems unsure as to the difference between an information security event and an information security incident. You attempt to explain the difference by providing examples.

Which three of the following scenarios can be defined as information security incidents?

## Options:

**A-** The organisation's malware protection software prevents a virus

**B-** A hard drive is used after its recommended replacement date

**C-** The organisation receives a phishing email

**D-** An employee fails to clear their desk at the end of their shift

**E-** A contractor who has not been paid deletes top management ICT accounts

**F-** An unhappy employee changes payroll records without permission

**G-** The organisation fails a third-party penetration test

**H-** The organisation's marketing data is copied by hackers and sold to a competitor

## Answer:

E, F, H

## Explanation:

According to ISO/IEC 27000:2018, which provides an overview and vocabulary of information security management systems, an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant1.An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security1. Therefore, based on this definition, three examples of information security incidents are:

A contractor who has not been paid deletes top management ICT accounts: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of access, data, or functionality for the top management.

An unhappy employee changes payroll records without permission: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in financial fraud, legal liability, or reputational damage for the organization.

The organisation's marketing data is copied by hackers and sold to a competitor: This is an example of an unwanted or unexpected information security event that has a significant probability of compromising business operations and threatening information security, as it may result in loss of confidentiality, competitive advantage, or customer trust for the organization.

The other options are not examples of information security incidents, but rather information security events that may or may not lead to incidents depending on their impact and severity. For example:

The organisation's malware protection software prevents a virus: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, as it is prevented by the malware protection software.

A hard drive is used after its recommended replacement date: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it fails or causes other problems.

The organisation receives a phishing email: This is an example of an identified occurrence of a network state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless it is opened or responded to by the recipient.

An employee fails to clear their desk at the end of their shift: This is an example of an identified occurrence of a service state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the desk contains sensitive or confidential information that is accessed by unauthorized persons.

The organisation fails a third-party penetration test: This is an example of an identified occurrence of a system state indicating a possible breach of information security policy or failure of safeguards, but it does not have a significant probability of compromising business operations and threatening information security, unless the penetration test reveals serious vulnerabilities that are exploited by malicious actors.

# Question 8

**Question Type:** MultipleChoice

You are an experienced ISMS auditor, currently providing support to an ISMS auditor in training who is carrying out her first initial certification audit. She asks you what she should be verifying when auditing an organisation's Information Security objectives. You ask her what she has included in her audit checklist and she provides the following replies.

Which three of these responses would you cause you concern in relation to conformity with ISO/IEC 27001:2022?

## Options:

**A-** I am going to check how each Information Security objective has been communicated to those who need to be aware of it in order for the objective to be achieved

**B-** I am going to check that top management have determined the Information Security objectives for the current year. If not, I will check that this task has been programmed to be completed

**C-** I am going to check that the Information Security objectives are written down on paper so that everyone is clear on what needs to be achieved, how it will be achieved, and by when it will be achieved

**D-** I am going to check that there is a process in place to periodically revisit Information Security objectives, with a view to amending or cancelling them if circumstances necessitate this

**E-** I am going to check that a completion date has been set for each objective and that there are no objectives with missing 'achieve by' dates

**F-** I am going to check that the necessary budget, manpower and materials to achieve each objective has been determined

**G-** I am going to check that all the Information Security objectives are measurable. If they are not measurable the organisation will not be able to track progress against them

## Answer:

B, C, E

## Explanation:

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 6.2 requires an organization to establish information security objectives at relevant functions and levels1.The objectives should be consistent with the information security policy; measurable (if practicable) or capable of being evaluated; monitored; communicated; updated as appropriate1. Therefore, when auditing an organization's information security objectives, an ISMS auditor should verify these aspects in accordance with the audit criteria.

Three responses from the ISMS auditor in training that would cause concern in relation to conformity with ISO/IEC 27001:2022 are:

I am going to check that top management have determined the Information Security objectives for the current year. If not, I will check that this task has been programmed to be completed: This response would cause concern because it implies that the auditor in training is not aware of the requirement to establish information security objectives at relevant functions and levels, not just at the top management level. It also implies that the auditor in training is willing to accept a delay or postponement in determining the information security objectives, which may affect the ISMS performance and effectiveness.

I am going to check that the Information Security objectives are written down on paper so that everyone is clear on what needs to be achieved, how it will be achieved, and by when it will be achieved: This response would cause concern because it implies that the auditor in training is not aware of the requirement to establish information security objectives that are measurable (if practicable) or capable of being evaluated, not just written down on paper. It also implies that the auditor in training is not aware of the flexibility and suitability of different media or formats for documenting and communicating information security objectives, such as electronic or digital records, posters, newsletters, etc.

I am going to check that a completion date has been set for each objective and that there are no objectives with missing 'achieve by' dates: This response would cause concern because it implies that the auditor in training is not aware of the requirement to establish information security objectives that are monitored, not just completed by a certain date. It also implies that the auditor in training is not aware of the possibility and necessity of updating information security objectives as appropriate, such as when changes occur in the internal or external context of the organization, or when new risks or opportunities arise.

The other responses from the ISMS auditor in training are acceptable and do not cause concern in relation to conformity with ISO/IEC 27001:2022. For example, checking how each Information Security objective has been communicated to those who need to be aware of it in order for the objective to be achieved is relevant to verifying the communication aspect of clause 6.2; checking that there is a process in place to periodically revisit Information Security objectives, with a view to amending or cancelling them if circumstances necessitate this is relevant to verifying the updating aspect of clause 6.2; checking that the necessary budget, manpower and materials to achieve each objective has been determined is relevant to verifying the planning aspect of clause 6.2; checking that all the Information Security objectives are measurable. If they are not measurable the organisation will not be able to track progress against them is relevant to verifying the measurability aspect of clause 6.2.Reference:ISO/IEC 27001:2022 - Information technology -- Security techniques -- Information security management systems -- Requirements

# Question 9

**Question Type:** **MultipleChoice**

You are preparing the audit findings. Select two options that are correct.

## Options:

**A-** There is an opportunity for improvement (OFI). The iLiirmation security incident training effectiveness can be improved. This is relevant to clause 7.2 and control A.6.3.

**B-** There is no nonconformance. The information security weaknesses, events, and incidents are reported. This conforms with clause 9.1 and control A.5.24.

**C-** There is no nonconformance. The information security handling training has performed, and its effectiveness was evaluated. This conforms with clause 7.2 and control A.6.3.

**D-** There is a nonconformity (NC). Based on sampling interview results, none of the interviewees were able to describe the incident management procedure reporting process including the role and responsibilities of personnel. This is not conforming with clause 9.1 and control A.5.24.

**E-** There is a nonconformity (NC). The information security incident training has failed. This is not conforming with clause 7.2 and control A.6.3.

**F-** There is an opportunity for improvement (OFI). The information security weaknesses, events, and madents are reported. This is relevant to clause 9.1 and control A.5.24.

## Answer:

A, D

## Explanation:

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), clause 7.2 requires an organization to determine the necessary competence of persons doing work under its control that affects its ISMS performance, and to provide training or take other actions to acquire or maintain the necessary competence1.Control A.6.3 requires an organization to ensure that all employees and contractors are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational policies and procedures in this respect2. Therefore, if an ISMS auditor finds that the information security incident training effectiveness can be improved, this indicates an opportunity for improvement (OFI) that is relevant to clause 7.2 and control A.6.3.

According to ISO/IEC 27001:2022, clause 9.1 requires an organization to monitor, measure, analyze and evaluate its ISMS performance and effectiveness1.Control A.5.24 requires an organization to define and apply procedures for reporting information security events and weaknesses2. Therefore, if an ISMS auditor finds that based on sampling interview results, none of the interviewees were able to describe the incident management procedure reporting process including the role and responsibilities of personnel, this indicates a nonconformity (NC) that is not conforming with clause 9.1 and control A.5.24.

The other options are not correct options for preparing the audit findings based on the given information. For example, there is no nonconformance if the information security weaknesses, events, and incidents are reported, as this conforms with clause 9.1 and control A.5.24; there is no nonconformance if the information security handling training has performed, and its effectiveness was evaluated, as this conforms with clause 7.2 and control A.6.3; there is no nonconformity if the information security incident training has failed, as this may not necessarily indicate a lack of conformity with clause 7.2 or control A.6.3; there is no opportunity for improvement if the information security weaknesses, events, and incidents are reported, as this is already conforming with clause 9.1 and control A.5.24.Reference:ISO/IEC 27001:2022 - Information technology -- Security techniques -- Information security management systems -- Requirements,ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls

# Question 10

**Question Type:** MultipleChoice

You are an experienced audit team leader guiding an auditor in training.

Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.

Select four controls from the following that would you expect the auditor in training to review.

You are an experienced audit team leader guiding an auditor in training,

Your team is currently conducting a third-party surveillance audit of an organisation that stores data on behalf of external clients. The auditor in training has been tasked with reviewing the TECHNOLOGICAL controls listed in the Statement of Applicability (SoA) and implemented at the site.

Select four controls from the following that would you expect the auditor in training to review.

## Options:

**A-** The development and maintenance of an information asset inventory

**B-** Rules for transferring information within the organisation and to other organisations

**C-** Confidentiality and nondisclosure agreements

**D-** How protection against malware is implemented

**E-** Access to and from the loading bay

**F-** The conducting of verification checks on personnel

**G-** Remote working arrangements

**H-** How information security has been addressed within supplier agreements

**I-** How the organisation evaluates its exposure to technical vulnerabilities

**J-** The organisation's business continuity arrangements

**K-** The organisation's arrangements for information deletion

**L-** Information security awareness, education and training

**M-** How access to source code and development tools are managed

**N-** The operation of the site CCTV and door control systems

**O-** The organisation's arrangements for maintaining equipment

**P-** How power and data cables enter the building

## Answer:

D, I, M, N

## Explanation:

According to ISO/IEC 27001:2022, which specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS), an organization should select and implement appropriate controls to achieve its information security objectives1.The controls should be derived from the results of risk assessment and risk treatment, and should be consistent with the Statement of Applicability (SoA), which is a document that identifies the controls that are applicable and necessary for the ISMS1.The controls can be selected from various sources, such as ISO/IEC 27002:2013, which provides a code of practice for information security controls2. Therefore, if an auditor in training has been tasked with reviewing the technological controls listed in the SoA and implemented at the site of an organization that stores data on behalf of external clients, four controls that would be expected to review are:

How protection against malware is implemented: This is a technological control that aims to prevent, detect and remove malicious software (such as viruses, worms, ransomware, etc.) that could compromise the confidentiality, integrity or availability of information or information systems2.This control is related to control A.12.2.1 of ISO/IEC 27002:20132.

How the organisation evaluates its exposure to technical vulnerabilities: This is a technological control that aims to identify and assess the potential weaknesses or flaws in information systems or networks that could be exploited by malicious actors or cause accidental failures2.This control is related to control A.12.6.1 of ISO/IEC 27002:20132.

How access to source code and development tools are managed: This is a technological control that aims to protect the intellectual property rights and integrity of software applications or systems that are developed or maintained by the organization or its external providers2.This control is related to control A.14.2.5 of ISO/IEC 27002:20132.

The operation of the site CCTV and door control systems: This is a technological control that aims to monitor and restrict physical access to the premises or facilities where information or information systems are stored or processed2.This control is related to control A.11.1.4 of ISO/IEC 27002:20132.

The other options are not examples of technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task. For example, the development and maintenance

of an information asset inventory (related to control A.8.1.1), rules for transferring information within the organization and to other organizations (related to control A.13.2.1), confidentiality and nondisclosure agreements (related to control A.13.2.4), verification checks on personnel (related to control A.7.1.2), remote working arrangements (related to control A.6.2.1), information security within supplier agreements (related to control A.15.1.1), business continuity arrangements (related to control A.17), information deletion (related to control A.8.3), information security awareness, education and training (related to control A.7.2), equipment maintenance (related to control A.11.2), and how power and data cables enter the building (related to control A.11) are not technological controls, but rather organizational, legal or procedural controls that may also be relevant for an ISMS audit, but are not within the scope of the auditor in training's task.Reference:ISO/IEC 27001:2022 - Information technology -- Security techniques -- Information security management systems -- Requirements,ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls