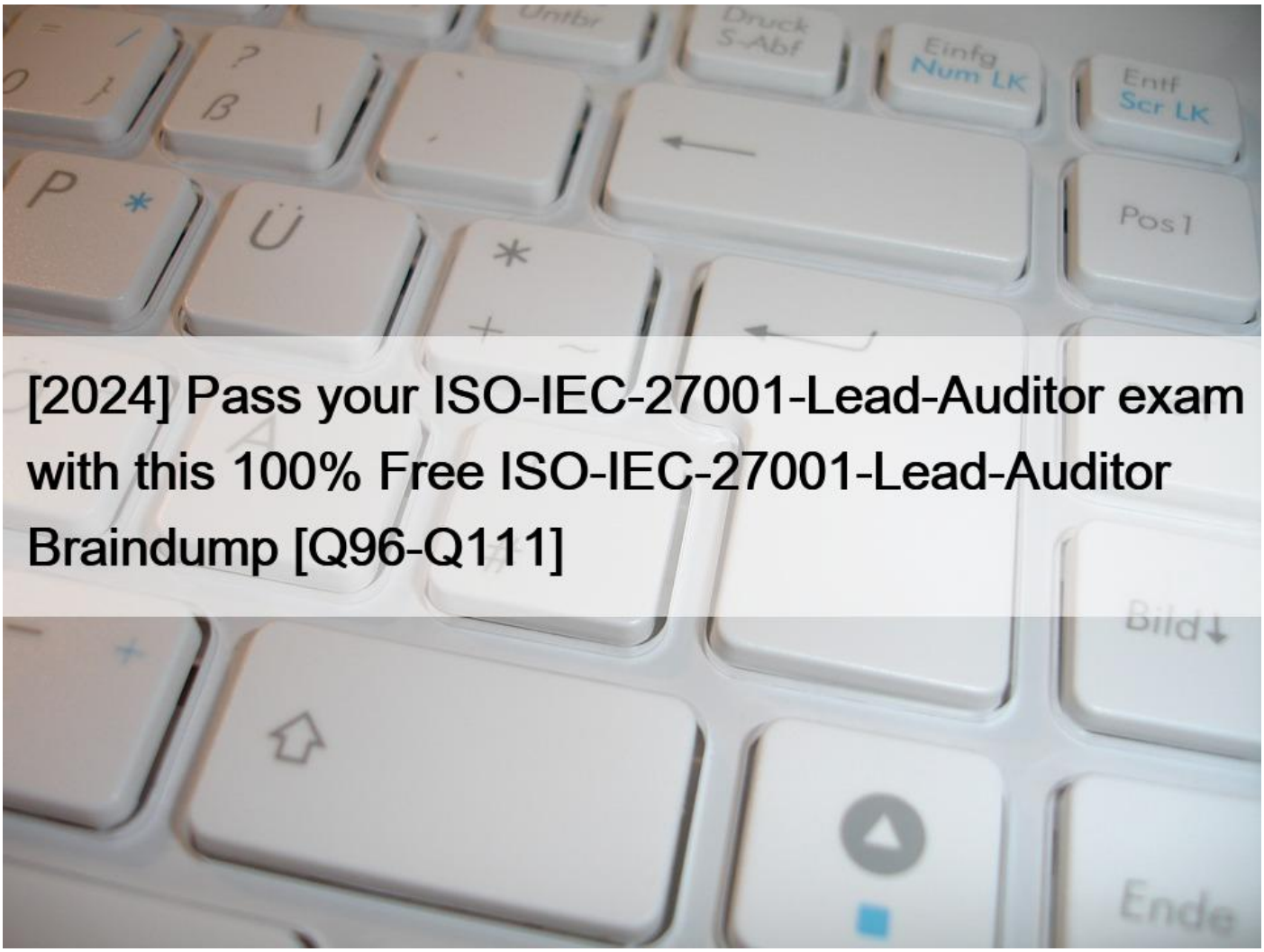
[2024 Pass your ISO-IEC-27001-Lead-Auditor exam with this 100% Free ISO-IEC-27001-Lead-Auditor Braindump [Q96-Q111



[2024] Pass your ISO-IEC-27001-Lead-Auditor exam with this 100% Free ISO-IEC-27001-Lead-Auditor Braindump
View All ISO-IEC-27001-Lead-Auditor Actual Exam Questions, Answers and Explanations for Free

The ISO-IEC-27001-Lead-Auditor certification exam is a comprehensive and rigorous examination that covers a wide range of topics related to information security management systems. ISO-IEC-27001-Lead-Auditor exam evaluates the candidate's knowledge and skills in areas such as risk assessment, risk management, security controls, auditing techniques, and communication with stakeholders. It also assesses their ability to lead and manage an audit team, including planning, executing, and reporting on an ISMS audit.

Q96. Which is the glue that ties the triad together
* Process
* People

* Collaboration
* Technology

Explanation

The triad refers to the three elements of information security: confidentiality, integrity and availability3. Technology is the glue that ties the triad together, as it provides the means to implement various controls and measures to protect information from unauthorized access, modification or loss3. References: ISO/IEC 27001:2022 Lead Auditor Training Course – BSI

Q97. In the event of an Information security incident, system users’ roles and responsibilities are to be observed, except:
* Report suspected or known incidents upon discovery through the Servicedesk
* Preserve evidence if necessary
* Cooperate with investigative personnel during investigation if needed
* Make the information security incident details known to all employees

Q98. Which department maintain’s contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications service providers depending on the service required.
* COO
* CISO
* CSM
* MRO

The department that maintains contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications service providers depending on the service required is CISO. CISO stands for Chief Information Security Officer. A CISO is a senior-level executive who is responsible for overseeing the information security strategy and governance of an organization. A CISO also leads the information security function and coordinates with other departments and stakeholders to ensure compliance with laws, regulations and standards related to information security. A CISO may also act as a liaison between the organization and external parties, such as law enforcement authorities or service providers, in case of incidents or investigations involving information security issues. ISO/IEC 27001:2022 requires the organization to assign top management roles and responsibilities for ensuring that information security objectives are established and achieved (see clause 5.3). Reference: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology – Security techniques – Information security management systems – Requirements, What is CISO?

Q99. In order to take out a fire insurance policy, an administration office must determine the value of the data that it manages.

Which factor is [b]not[/b] important for determining the value of data for an organization?
* The content of data.
* The degree to which missing, incomplete or incorrect data can be recovered.
* The indispensability of data for the business processes.
* The importance of the business processes that make use of the data.

Q100. A planning process that introduced the concept of planning as a cycle that forms the basis for continuous improvement is called:
* time based planning.
* plan, do, check, act.
* planning for continuous improvement.
* RACI Matrix

Q101. Stages of Information
* creation, evolution, maintenance, use, disposition
* creation, use, disposition, maintenance, evolution
* creation, distribution, use, maintenance, disposition

* creation, distribution, maintenance, disposition, use

The stages of information are creation, distribution, use, maintenance, and disposition. These are the phases that information goes through during its lifecycle, from the moment it is generated to the moment it is destroyed or archived. Each stage of information has different security requirements and risks, and should be managed accordingly. Creation, evolution, maintenance, use, and disposition are not the correct stages of information, as evolution is not a distinct stage, but a process that can occur in any stage. Creation, use, disposition, maintenance, and evolution are not the correct stages of information, as they are not in the right order. Creation, distribution, maintenance, disposition, and use are not the correct stages of information, as they are not in the right order.
References: : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 32. : [ISO/IEC 27001 LEAD AUDITOR – PECB], page 12.

Q102. Which of the following does a lack of adequate security controls represent?

* Asset
* Vulnerability
* Impact
* Threat

Q103. Cabling Security is associated with Power, telecommunication and network cabling carrying information are protected from interception and damage.

* True
* False

Q104. You are performing an ISMS audit at a residential nursing home called ABC that provides healthcare services.

You find all nursing home residents wear an electronic wristband for monitoring their location, heartbeat, and blood pressure always. You learned that the electronic wristband automatically uploads all data to the artificial intelligence (AI) cloud server for healthcare monitoring and analysis by healthcare staff.

To verify the scope of ISMS, you interview the management system representative (MSR) who explains that the ISMS scope covers an outsourced data center.

Select three options for the audit evidence you need to find to verify the scope of the ISMS.

* The auditee has identified the resident’s needs and expectations on the facility and environmental safety
* The auditee has ISO 9001 certification
* The auditee has identified the governmental authorities’ needs and expectations on healthcare services and patient data handling
* The auditee has identified the resident’s needs and expectations on how they should protect the resident’s personal data
* The auditee has identified the resident’s needs and expectations on the comfort facility, medical professional’s competence, and clean environment
* The auditee has identified the resident’s needs and expectations on healthcare medical treatment services
* The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located
* The auditee is considering the purchase of a healthcare monitoring app from an external software company

Explanation

According to ISO 27001:2022 clause 4.3, the organisation shall determine the scope of the information security management system (ISMS) by considering the internal and external issues, the requirements of interested parties, and the interfaces and dependencies with other organisations12 In this case, the ISMS scope covers an outsourced data center that hosts the artificial intelligence (AI) cloud server for healthcare monitoring and analysis of the residents’ data. Therefore, the audit evidence you need to find to verify the scope of the ISMS should include:

* The auditee has identified the governmental authorities’ needs and expectations on healthcare services and patient data handling. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to comply with the relevant laws and regulations regarding the quality, safety, and privacy of healthcare services and patient data12

* The auditee has identified the resident’s needs and expectations on how they should protect the resident’s personal data. This is an external issue and an interested party requirement that affects the ISMS scope, as the auditee has to ensure the confidentiality, integrity, and availability of the resident’s personal data that is collected, processed, and stored by the electronic wristband and the AI cloud server12

* The IT service agreement with the data center where the artificial intelligence (AI) cloud server is located. This is an interface and dependency with another organisation that affects the ISMS scope, as the auditee has to control the externally provided processes, products, and services that are relevant to the ISMS, and to implement appropriate contractual requirements related to information security12 The following options are not relevant or sufficient for verifying the scope of the ISMS:

* The auditee has identified the resident’s needs and expectations on the facility and environmental safety.

This is an external issue and an interested party requirement, but it does not affect the ISMS scope, as it is not related to information security12

* The auditee has ISO 9001 certification. This is an indication of the auditee’s quality management system, but it does not verify the scope of the ISMS, as it is not related to information security12

* The auditee has identified the resident’s needs and expectations on the comfort facility, medical professional’s competence, and clean environment. These are external issues and interested party requirements, but they do not affect the ISMS scope, as they are not related to information security12

* The auditee has identified the resident’s needs and expectations on healthcare medical treatment services. These are external issues and interested party requirements, but they do not verify the scope of the ISMS, as they are not specific to information security12

* The auditee is considering the purchase of a healthcare monitoring app from an external software company. This is a potential change that may affect the ISMS scope in the future, but it does not verify the current scope of the ISMS, as it is not yet implemented or controlled12 References:

1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1
2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

Q105. Which option below about the ISMS scope is correct?
* ISMS scope should be available as documented information
* ISMS scope should ensure continual improvement
* ISMS scope should be compatible with the strategic orientation of the organization

According to ISO/IEC 27001, the scope of an ISMS must be defined and documented. This documentation should include the boundaries and applicability of the information security management system, which helps in defining what information, locations, and assets are covered under the ISMS.

References: ISO/IEC 27001:2013 Standard, Clause 4.3 (Determining the scope of the information security management system)

Q106. The following are definitions of Information, except:
* accurate and timely data
* specific and organized data for a purpose

* mature and measurable data
* can lead to understanding and decrease in uncertainty

Explanation

The definition of information that is not correct is C: mature and measurable data. This is not a valid definition of information, as information does not have to be mature or measurable to be considered as such. Information can be any data that has meaning or value for someone or something in a certain context. Information can be subjective, qualitative, incomplete or uncertain, depending on how it is interpreted or used. Mature and measurable data are characteristics that may apply to some types of information, but not all. The other definitions of information are correct, as they describe different aspects of information, such as accuracy and timeliness (A), specificity and organization (B), and understanding and uncertainty reduction (D). ISO/IEC

27001:2022 defines information as “any data that has meaning” (see clause 3.25). References: CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course, ISO/IEC 27001:2022 Information technology

– Security techniques – Information security management systems – Requirements, What is Information?

Q107. Which is the glue that ties the triad together
* Process
* People
* Collaboration
* Technology

Q108. You are preparing the audit findings. Select two options that are correct.
* 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.
* There is no nonconformance. The information security weaknesses, events, and incidents are reported.

This conforms with clause 9.1 and control A.5.24.
* 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.
* 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.
* 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.
* 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.

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. References: 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

Q109. You are an experienced ISMS audit team leader providing guidance to an ISMS auditor in training. They have been asked to carry out an assessment of external providers and have prepared a checklist containing the following activities. They have asked you to review their checklist to confirm that the actions they are proposing are appropriate.

The audit they have been invited to participate in is a third-party surveillance audit of a data centre . The data centre agent is part of a wider telecommunication group. Each data centre within the group operates its own ISMS and holds its own certificate.

Select three options that relate to ISO/IEC 27001:2022’s requirements regarding external providers.
* I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group
* I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services
* I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information
* I will limit my audit activity to externally provided processes as there is no need to audit externally provided products of services
* I will ensure the organization is regularly monitoring, reviewing and evaluating external provider performance
* I will ensure the organization is has determined the need to communicate with external providers regarding the ISMS
* I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes
* I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest

A. I will check the other data centres are treated as external providers, even though they are part of the same telecommunication group. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to ensure that externally provided processes, products or services that are relevant to the information security management system are controlled. Externally provided processes, products or services are those that are provided by any external party, regardless of the degree of its relationship with the organisation. Therefore, the other data centres within the same telecommunication group should be treated as external providers and subject to the same controls as any other external provider12

B. I will ensure external providers have a documented process in place to notify the organisation of any risks arising from the use of its products or services. This is appropriate because clause 8.1.4 of ISO

27001:2022 requires the organisation to implement appropriate contractual requirements related to information security with external providers. One of the contractual requirements could be the obligation of the external provider to notify the organisation of any risks arising from the use of its products or services, such as security incidents, vulnerabilities, or changes that could affect the information security of the organisation. The external provider should have a documented process in place to ensure that such notification is timely, accurate, and complete12

E. I will ensure the organisation is regularly monitoring, reviewing and evaluating external provider performance. This is appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to monitor, review and evaluate the performance and effectiveness of the externally provided processes, products or services. The organisation should have a process in place to measure and verify the conformity and suitability of the external provider’s deliverables and activities, and to provide feedback and improvement actions as necessary. The organisation should also maintain records of the monitoring, review and evaluation results12

F. I will ensure the organisation has determined the need to communicate with external providers regarding the ISMS. This is appropriate because clause 7.4.2 of ISO 27001:2022 requires the organisation to determine the need for internal and external communications relevant to the information security management system, including the communication with external providers. The organisation should define the purpose, content, frequency, methods, and responsibilities for such communication, and ensure that it is consistent with the information security policy and objectives. The organisation should also retain documented information of the communication as evidence of its implementation12 The following activities are not appropriate for the assessment of external providers according to ISO

27001:2022:

C. I will ensure that the organisation has a reserve external provider for each process it has identified as critical to preservation of the confidentiality, integrity and accessibility of its information. This is not appropriate because ISO 27001:2022 does not require the organisation to have a reserve external provider for each critical process. The organisation may choose to have a contingency plan or a backup solution in case of failure or disruption of the external provider, but this is not a mandatory requirement. The organisation should assess the risks and opportunities associated with the external provider and determine the appropriate treatment options, which may or may not include having a reserve external provider12

D. I will limit my audit activity to externally provided processes as there is no need to audit externally provided products or services. This is not appropriate because clause 8.1.4 of ISO 27001:2022 requires the organisation to control the externally provided processes, products or services that are relevant to the information security management system. Externally provided products or services may include software, hardware, data, or cloud services that could affect the information security of the organisation. Therefore, the audit activity should cover both externally provided processes and products or services, as applicable12

G. I will ensure that top management have assigned roles and responsibilities for those providing external ISMS processes as well as internal ISMS processes. This is not appropriate because clause 5.3 of ISO 27001:2022 requires the top management to assign the roles and responsibilities for the information security management system within the organisation, not for the external providers. The external providers are responsible for assigning their own roles and responsibilities for the processes, products or services they provide to the organisation. The organisation should ensure that the external providers have adequate competence and awareness for their roles and responsibilities, and that they are contractually bound to comply with the information security requirements of the organisation12

H. I will ensure that the organisation ranks its external providers and allocates the majority of its work to those providers who are rated the highest. This is not appropriate because ISO 27001:2022 does not require the organisation to rank its external providers or to allocate its work based on such ranking. The organisation may choose to evaluate and compare the performance and effectiveness of its external providers, but this is not a mandatory requirement. The organisation should select and use its external providers based on the information security criteria and objectives that are relevant to the organisation12 References:

1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1
2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

Q110. A key audit process is the way auditors gather information and determine the findings’ characteristics. Put the actions listed in the correct order to complete this process. The last one has been done for you.

A key audit process is the way auditors gather information and determine the findings' characteristics. Put the actions listed in the correct order to
for you.

Actions

1. Determine source of information
2. Collect by means of appropriate sampling
3. [ ]
4. [ ]
5. [ ]
6. [ ]
7. Audit conclusions

To complete the sentence with the best words that describe the nonconformity, click on the blank section you want to complete so that it is highlig
from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Audit evidence | Reviewing | Evaluating against audit criteria | Audit findings

A key audit process is the way auditors gather information and determine the findings' characteristics. Put the actions listed in the correct order to
for you.

Actions

1. Determine source of information
2. Collect by means of appropriate sampling
3. Reviewing
4. Audit evidence
5. Evaluating against audit criteria
6. Audit findings
7. Audit conclusions

To complete the sentence with the best words that describe the nonconformity, click on the blank section you want to complete so that it is highlig
from the options below. Alternatively, you may drag and drop the option to the appropriate blank section.

Audit evidence | Reviewing | Evaluating against audit criteria | Audit findings

Explanation:

* Determine source of information

* Collect by means of appropriate sampling

* Reviewing

* Audit evidence

* Evaluating against audit criteria

* Audit findings

* Audit conclusions

The reviewing step involves checking the accuracy, completeness, and relevance of the collected information.

The audit evidence step involves documenting the information in a verifiable and traceable manner. The evaluating against audit criteria step involves comparing the audit evidence with the requirements of the ISO

27001 standard and the organization’s own policies and objectives. The audit findings step involves identifying any nonconformities, weaknesses, or opportunities for improvement in the ISMS. The audit conclusions step involves summarizing the audit results and providing recommendations for corrective actions or enhancements.

Q111. 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. Referencing the scenario, which three of the following Annex A controls would you expect the auditee to have implemented when you conduct the follow-up audit?
* 5.11 Return of assets
* 5.13 Labelling of information
* 5.3 Segregation of duties
* 5.32 Intellectual property rights
* 5.34 Privacy and protection of personal identifiable information (PII)
* 5.6 Contact with special interest groups
* 6.3 Information security awareness, education, and training
* 6.4 Disciplinary process

Explanation

The three Annex A controls that you would expect the auditee to have implemented when you conduct the follow-up audit are:

B: 5.13 Labelling of information

E: 5.34 Privacy and protection of personal identifiable information (PII) G: 6.3 Information security awareness, education, and training B: This control requires the organisation to label information assets in accordance with the information classification scheme, and to handle them accordingly12. This control is relevant for the auditee because it could help them to avoid misaddressing labels and sending parcels to wrong destinations, which could compromise the confidentiality, integrity, and availability of the information assets. By labelling the information assets correctly, the auditee could also ensure that they are delivered to the intended recipients and that they are protected from unauthorized access, use, or disclosure.

E: This control requires the organisation to protect the privacy and the rights of individuals whose personal identifiable information (PII) is processed by the organisation, and to comply with the applicable legal and contractual obligations13. This control is relevant for the auditee because it could help them to prevent the unauthorized use of residents’ personal data by a supplier, which could violate the privacy and the rights of the residents and their family members, and expose the auditee to legal and reputational risks. By protecting the PII of the residents and their family members, the auditee could also enhance their trust and satisfaction, and avoid complaints and disputes.

G: This control requires the organisation to ensure that all employees and contractors are aware of the information security policy, their roles and responsibilities, and the relevant information security procedures and controls14. This control is relevant for the auditee because it could help them to improve the information security culture and behaviour of their staff, and to reduce the human errors and negligence that could lead to information security incidents. By providing information security awareness, education, and training to their staff, the auditee could also increase their competence and performance, and ensure the effectiveness and efficiency of the information security processes and controls.

References:

1: ISO/IEC 27001:2022 – Information technology – Security techniques – Information security management systems – Requirements, Annex A 2: ISO/IEC 27002:2022 – Information technology – Security techniques

– Code of practice for information security controls, clause 8.2.1 3: ISO/IEC 27002:2022 – Information technology – Security techniques – Code of practice for information security controls, clause 18.1.4 4:

ISO/IEC 27002:2022 – Information technology – Security techniques – Code of practice for information security controls, clause 7.2.2