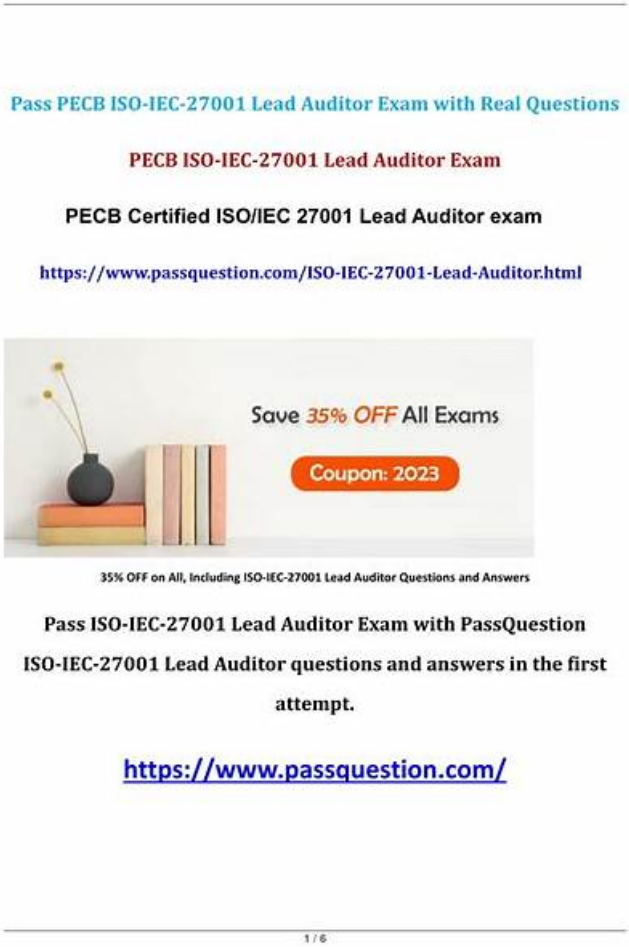
Real PECB ISO-IEC-27001-Lead-Auditor Exam Questions with Verified Answers



P.S. Free 2026 PECB ISO-IEC-27001-Lead-Auditor dumps are available on Google Drive shared by DumpsValid: https://drive.google.com/open?id=14yDkln4e84LREuEMVPIMPXFM8QjeUqDR

As is known to us, getting the newest information is very important for all people to pass the exam and get the certification in the shortest time. In order to help all customers gain the newest information about the ISO-IEC-27001-Lead-Auditor exam, the experts and professors from our company designed the best PECB Certified ISO/IEC 27001 Lead Auditor exam test guide. The experts will update the system every day. If there is new information about the exam, you will receive an email about the newest information about the ISO-IEC-27001-Lead-Auditor learning dumps. We can promise that you will never miss the important information about the exam.

The quality of DumpsValid product is very good and also have the fastest update rate. If you purchase the training materials we provide, you can pass PECB Certification ISO-IEC-27001-Lead-Auditor Exam successfully.

>> Reliable ISO-IEC-27001-Lead-Auditor Test Tutorial <<

Trustworthy Reliable ISO-IEC-27001-Lead-Auditor Test Tutorial Offers Candidates Pass-Sure Actual PECB PECB Certified ISO/IEC 27001 Lead Auditor exam Exam Products

The PECB Certified ISO/IEC 27001 Lead Auditor exam practice exam material is available in three different formats i.e PECB ISO-IEC-27001-Lead-Auditor dumps PDF format, web-based practice test software, and desktop ISO-IEC-27001-Lead-Auditor practice exam software. PDF format is pretty much easy to use for the ones who always have their smart devices and love to prepare for ISO-IEC-27001-Lead-Auditor Exam from them. Applicants can also make notes of printed PECB Certified ISO/IEC 27001 Lead Auditor exam (ISO-IEC-27001-Lead-Auditor) exam material so they can use it anywhere in order to pass PECB ISO-IEC-27001-Lead-Auditor Certification with a good score.

PECB Certified ISO/IEC 27001 Lead Auditor certification exam is designed for individuals who have a minimum of five years of professional experience in information security management, including two years of experience in auditing. PECB Certified ISO/IEC 27001 Lead Auditor exam certification exam covers various topics such as the principles, concepts, and standards of information security management, the audit process, audit techniques, and reporting. It also requires candidates to demonstrate their ability to lead an audit team, plan and conduct an audit, and communicate effectively with stakeholders.

PECB Certified ISO/IEC 27001 Lead Auditor exam Sample Questions (Q127-Q132):

NEW QUESTION # 127
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.

- A. Interview the reception personnel to make sure all visitor and employee bags are checked before entering the nursing home
- B. Review the asset register to make sure all company's mobile devices are registered
- C. Interview top management to verify their involvement in establishing the information security policy and the information security objectives
- D. Review the internal audit report to make sure the IT department has been audited
- E. Interview the supplier of the devices to make sure they are aware of the ISMS policy
- F. Review visitors' register book to make sure no visitor can have their personal mobile phone in the nursing home
- G. Review the asset register to make sure all personal mobile devices are registered
- H. Sampling some mobile devices from on-duty medical staff and validate the mobile device information with the asset register

Answer: B,D,H

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

NEW QUESTION # 128
You are an ISMS audit team leader who has been assigned by your certification body to carry out a follow-up audit of a client. You are preparing your audit plan for this audit.
Which two of the following statements are true?

- A. Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement
- B. Opportunities for improvement should be verified first, followed by corrections and finally corrective actions
- C. Corrections should be verified first, followed by corrective actions and finally opportunities for improvement
- D. Verification should focus on whether any action undertaken has been undertaken effectively
- E. Verification should focus on whether any action undertaken taken has been undertaken efficiently
- F. Verification should focus on whether any action undertaken is complete

Answer: D,F

Explanation:
According to ISO 27001:2022 clause 9.1.2, the organisation shall conduct internal audits at planned intervals to provide information on whether the information security management system conforms to the organisation's own requirements, the requirements of ISO 27001:2022, and is effectively implemented and maintained12 According to ISO 27001:2022 clause 10.1, the organisation shall react to the nonconformities and take action, as applicable, to control and correct them and deal with the consequences. The organisation shall also evaluate the need for action to eliminate the causes of nonconformities, in order to prevent recurrence or occurrence.
The organisation shall implement any action needed, review the effectiveness of any corrective action taken, and make changes to the information security management system, if necessary12 A follow-up audit is a type of internal audit that is conducted after a previous audit to verify whether the nonconformities and corrective actions have been addressed and resolved, and whether the information security management system has been improved12 Therefore, the following statements are true for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken is complete. This means that the auditor should check whether the organisation has implemented all the planned actions to correct and prevent the nonconformities, and whether the actions have been documented and communicated as required12
* Verification should focus on whether any action undertaken has been undertaken effectively. This means that the auditor should check whether the organisation has achieved the intended results and objectives of the actions, and whether the actions have eliminated or reduced the nonconformities and their causes and consequences12 The following statements are false for preparing a follow-up audit plan:
* Verification should focus on whether any action undertaken has been undertaken efficiently. This is false because efficiency is not a criterion for verifying the actions taken to address the nonconformities and corrective actions. Efficiency refers to the optimal use of resources to achieve the desired outcomes, but it is not a requirement of ISO 27001:2022. The auditor should focus on the

effectiveness and completeness of the actions, not on the efficiency12
* Corrections should be verified first, followed by corrective actions and finally opportunities for improvement. This is false because there is no prescribed order for verifying the corrections, corrective actions, and opportunities for improvement. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Opportunities for improvement should be verified first, followed by corrections and finally corrective actions. This is false because there is no prescribed order for verifying the opportunities for improvement, corrections, and corrective actions. The auditor should verify all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to verify the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12
* Corrective actions should be reviewed first, followed by corrections and finally opportunities for improvement. This is false because there is no prescribed order for reviewing the corrective actions, corrections, and opportunities for improvement. The auditor should review all the actions taken by the organisation, regardless of their sequence or priority. The auditor may choose to review the actions based on their relevance, significance, or impact, but this is not a mandatory requirement12 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

NEW QUESTION # 129
Select the correct sequence for the information security risk assessment process in an ISMS.
To complete the sequence 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 options to the appropriate blank

Answer:

Explanation:
Explanation:
A group of black text Description automatically generated
According to ISO 27001:2022, the standard for information security management systems (ISMS), the correct sequence for the information security risk assessment process is as follows:
Establish information security criteria
Identify the information security risks
Analyse the information security risks
Evaluate the information security risks
The first step is to establish the information security criteria, which include the risk assessment methodology, the risk acceptance criteria, and the risk evaluation criteria. These criteria define how the organization will perform the risk assessment, what level of risk is acceptable, and how the risks will be compared and prioritized.
The second step is to identify the information security risks, which involve identifying the assets, threats, vulnerabilities, and existing controls that are relevant to the ISMS. The organization should also identify the potential consequences and likelihood of each risk scenario.
The third step is to analyse the information security risks, which involve estimating the level of risk for each risk scenario based on the criteria established in the first step. The organization should also consider the sources of uncertainty and the confidence level of the risk estimation.
The fourth step is to evaluate the information security risks, which involve comparing the estimated risk levels with the risk acceptance criteria and determining whether the risks are acceptable or need treatment. The organization should also prioritize the risks based on the risk evaluation criteria and the objectives of the ISMS.
References: ISO 27001:2022 Clause 6.1.2 Information security risk assessment, ISO 27001 Risk Assessment & Risk Treatment: The Complete Guide - Advisera, ISO 27001 Risk Assessment: 7 Step Guide - IT Governance UK Blog

NEW QUESTION # 130
The data center at which you work is currently seeking ISO/IEC27001:2022 certification. In preparation for your initial certification visit a number of internal audits have been carried out by a colleague working at another data centre within your Group. They secured their ISO/IEC 27001:2022 certificate earlier in the year.
You have just qualified as an Internal ISMS auditor and your manager has asked you to review the audit process and audit findings as a final check before the external Certrfication Body arrives.
Which six of the following would cause you concern in respect of conformity to ISO/IEC 27001:2022 requirements?

- A. Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme
- B. Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's

intranet

- C. The audit programme does not take into account the relative importance of information security processes
- D. The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022
- E. Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date
- F. The audit programme shows management reviews taking place at irregular intervals during the year
- G. The audit process states the results of audits will be made available to 'relevant' managers, not top management
- H. The audit programme does not reference audit methods or audit responsibilities
- I. Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes
- J. The audit programme does not take into account the results of previous audits

Answer: A,C,E,F,I,J

Explanation:
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 9.3 requires top management to review the organization's ISMS at planned intervals to ensure its continuing suitability, adequacy and effectiveness1. Clause 9.2 requires the organization to conduct internal audits at planned intervals to provide information on whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022, and is effectively implemented and maintained1. Therefore, when reviewing the audit process and audit findings as a final check before the external certification body arrives, an internal ISMS auditor should verify that these clauses are met in accordance with the audit criteria.
Six of the following statements would cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
* The audit programme shows management reviews taking place at irregular intervals during the year:
This statement would cause concern because it implies that the organization is not conducting management reviews at planned intervals, as required by clause 9.3. This may affect the ability of top management to ensure the continuing suitability, adequacy and effectiveness of the ISMS.
* The audit programme does not take into account the relative importance of information security processes: This statement would cause concern because it implies that the organization is not applying a risk-based approach to determine the audit frequency, methods, scope and criteria, as recommended by ISO 19011:2018, which provides guidelines for auditing management systems2. This may affect the ability of the organization to identify and address the most significant risks and opportunities for its ISMS.
* Although the scope for each internal audit has been defined, there are no audit criteria defined for the audits carried out to date: This statement would cause concern because it implies that the organization is not establishing audit criteria for each internal audit, as required by clause 9.2. Audit criteria are the set of policies, procedures or requirements used as a reference against which audit evidence is compared2.
Without audit criteria, it is not possible to determine whether the ISMS conforms to its own requirements and those of ISO/IEC 27001:2022.
* Audit reports to date have used key performance indicator information to focus solely on the efficiency of ISMS processes: This statement would cause concern because it implies that the organization is not evaluating the effectiveness of ISMS processes, as required by clause 9.1. Effectiveness is the extent to which planned activities are realized and planned results achieved2. Efficiency is the relationship between the result achieved and the resources used2. Both aspects are important for measuring and evaluating ISMS performance and improvement.
* The audit programme does not take into account the results of previous audits: This statement would cause concern because it implies that the organization is not using the results of previous audits as an input for planning and conducting subsequent audits, as recommended by ISO 19011:20182. This may affect the ability of the organization to identify and address any recurring or unresolved issues or nonconformities related to its ISMS.
* Top management commitment to the ISMS will not be audited before the certification visit, according to the audit programme: This statement would cause concern because it implies that the organization is not verifying that top management demonstrates leadership and commitment with respect to its ISMS, as required by clause 5.1. This may affect the ability of top management to ensure that the ISMS policy and objectives are established and compatible with the strategic direction of the organization; that roles, responsibilities and authorities for relevant roles are assigned and communicated; that resources needed for the ISMS are available; that communication about information security matters is established; that continual improvement of the ISMS is promoted; that other relevant management reviews are aligned with those of information security; and that support is provided to other relevant roles1.
The other statements would not cause concern in respect of conformity to ISO/IEC 27001:2022 requirements:
* Audit reports are not held in hardcopy (i.e. on paper). They are only stored as ".POF documents on the organisation's intranet: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific format or media for documenting or storing audit reports, as long as they are controlled according to clause 7.5.
* The audit programme mandates auditors must be independent of the areas they audit in order to satisfy the requirements of ISO/IEC 27001:2022: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC

27001:2022 requirements. The standard does not prescribe any specific requirement for auditor independence, as long as the audit is conducted objectively and impartially, in accordance with ISO 19011:20182.
* The audit programme does not reference audit methods or audit responsibilities: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for referencing audit methods or audit responsibilities in the audit programme, as long as they are defined and documented according to ISO 19011:20182.
* The audit process states the results of audits will be made available to 'relevant' managers, not top management: This statement would not cause concern because it does not imply any nonconformity with ISO/IEC 27001:2022 requirements. The standard does not prescribe any specific requirement for communicating the results of audits to top management, as long as they are reported to the relevant parties and used as an input for management review, according to clause 9.3.
References: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, ISO 19011:2018 - Guidelines for auditing management systems

NEW QUESTION # 131
You are performing an ISO 27001 ISMS surveillance audit at a residential nursing home, ABC Healthcare Services. ABC uses a healthcare mobile app designed and maintained by a supplier, WeCare, to monitor residents' well-being. During the audit, you learn that 90% of the residents' family members regularly receive medical device advertisements from WeCare, by email and SMS once a week. The service agreement between ABC and WeCare prohibits the supplier from using residents' personal data. ABC has received many complaints from residents and their family members.
The Service Manager says that the complaints were investigated as an information security incident which found that they were justified.
Corrective actions have been planned and implemented according to the nonconformity and corrective action management procedure.
You write a nonconformity "ABC failed to comply with information security control A.5.34 (Privacy and protection of PII) relating to the personal data of residents' and their family members. A supplier, WeCare, used residents' personal information to send advertisements to family members." Select three options of the corrections and corrective actions listed that you would expect ABC to make in response to the nonconformity.

- A. ABC trains all staff on the importance of maintaining information security protocols.
- B. ABC periodically monitors compliance with all applicable legislation and contractual requirements involving third parties.
- C. ABC discontinues the use of the ABC Healthcare mobile app.
- D. ABC takes legal action against WeCare for breach of contract.
- E. ABC introduces background checks on information security performance for all suppliers.
- F. ABC confirms that information security control A.5.34 is contained in the Statement of Applicability (SoA).
- G. ABC cancels the service agreement with WeCare.
- H. ABC asks an ISMS consultant to test the ABC Healthcare mobile app for protection against cyber-crime.

Answer: B,E,G

Explanation:
The three options of the corrections and corrective actions listed that you would expect ABC to make in response to the nonconformity are:
B. ABC cancels the service agreement with WeCare.
E. ABC introduces background checks on information security performance for all suppliers.
F. ABC periodically monitors compliance with all applicable legislation and contractual requirements involving third parties.
B. This option is a possible correction and corrective action that ABC could take to address the nonconformity. A correction is the action taken to eliminate a detected nonconformity, while a corrective action is the action taken to eliminate the cause of a nonconformity and to prevent its recurrence1. By cancelling the service agreement with WeCare, ABC could stop the unauthorized use of residents' personal data and protect their privacy and rights. This could also prevent further complaints and legal issues from the residents and their family members. However, this option may also have some drawbacks, such as the loss of a service provider, the need to find an alternative solution, and the potential impact on the residents' well-being.
E. This option is a possible corrective action that ABC could take to address the nonconformity. By introducing background checks on information security performance for all suppliers, ABC could ensure that they select and work with reliable and trustworthy partners who respect the confidentiality, integrity, and availability of the information they handle. This could also help ABC to comply with information security control A.15.1.1 (Information security policy for supplier relationships), which requires the organisation to agree and document information security requirements for mitigating the risks associated with supplier access to the organisation's assets2.
F. This option is a possible corrective action that ABC could take to address the nonconformity. By periodically monitoring compliance with all applicable legislation and contractual requirements involving third parties, ABC could verify that the suppliers are fulfilling their obligations and responsibilities regarding information security. This could also help ABC to comply with information

security control A.18.1.1 (Identification of applicable legislation and contractual requirements), which requires the organisation to identify, document, and keep up to date the relevant legislative, regulatory, contractual, and other requirements to which the organisation is subject3.
References:
1: ISO 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary, clause 3.9 and 3.10 2: ISO/IEC 27001:2022 - Information technology
- Security techniques - Information security management systems - Requirements, Annex A, control
A.15.1.1 3: ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements, Annex A, control A.18.1.1

NEW QUESTION # 132
.....

Our ISO-IEC-27001-Lead-Auditor learning guide is very efficient tool in the world. As is known to us, in our modern world, everyone is looking for to do things faster, better, smarter, so it is no wonder that productivity hacks are incredibly popular. So we must be aware of the importance of the study tool. In order to promote the learning efficiency of our customers, our ISO-IEC-27001-Lead-Auditor Training Materials were designed by a lot of experts from our company. You can totally rely on our ISO-IEC-27001-Lead-Auditor study materials.

myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, contusiones.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

What's more, part of that DumpsValid ISO-IEC-27001-Lead-Auditor dumps now are free: https://drive.google.com/open?id=14yDkln4e84LREuEMVPIMPXFM8QjeUqDR