

PECB.ISO-IEC-27001-Lead-Implementer.v2024-02-19.q71

Exam Code:	ISO-IEC-27001-Lead-Implementer
Exam Name:	PECB Certified ISO/IEC 27001 Lead Implementer Exam
Certification Provider:	PECB
Free Question Number:	71
Version:	v2024-02-19
# of views:	911
# of Questions views:	710
https://www.freepdfdumps.com/PECB.ISO-IEC-27001-Lead-Implementer.v2024-02-19.q71.html	

NEW QUESTION: 1

What risk treatment option has Company A implemented if it has required from its employees the change of email passwords at least once every 60 days?

- A. Risk avoidance
- B. Risk retention
- C. Risk modification

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 2

FinanceX, a well-known financial institution, uses an online banking platform that enables clients to easily and securely access their bank accounts. To log in, clients are required to enter the one-time authorization code sent to their smartphone. What can be concluded from this scenario?

- A. FinanceX has implemented a securityControl that ensures the confidentiality of information
- B. FinanceX has implemented an integrity control that avoids the involuntary corruption of data
- C. FinanceX has incorrectly implemented a security control that could become a vulnerability

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 3

What supports the continual improvement of an ISMS?

- A. The update of documented information
- B. The update of action plans
- C. The update of external audit reports

Answer: A ([LEAVE A REPLY](#))**Explanation**

According to the ISO/IEC 27001:2022 standard, the organization should establish, implement and maintain a process to manage changes that affect the information security management system (ISMS) and to continually improve the suitability, adequacy and effectiveness of the ISMS (section 8.1.3 and 10.2). The standard also states that the organization should update the documented information of the ISMS as necessary to reflect the changes and the results of the improvement process (section 8.1.3.2 and 10.2.2). Therefore, the update of documented information supports the continual improvement of the ISMS by ensuring that the ISMS is aligned with the current and future needs and expectations of the organization and its interested parties.

References:

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements¹ ISO/IEC 27001 Lead Implementer Info Kit Continual Improvement For ISO 27001 Requirement 10.22

NEW QUESTION: 4

Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB, a document model database that offers high availability, scalability, and flexibility.

Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.

Fortunately, Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions. To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.

Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Socket Inc. has implemented a control for the effective use of cryptography and cryptographic key management. Is this compliant with ISO/IEC 27001? Refer to scenario 3.

A. No, the control should be implemented only for defining rules for cryptographic key management

B. Yes, the control for the effective use of the cryptography can include cryptographic key management

C. No, because the standard provides a separate control for cryptographic key management

Answer: B (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001:2022, Annex A.8.24, the control for the effective use of cryptography is intended to ensure proper and effective use of cryptography to protect the confidentiality, authenticity, and/or integrity of information. This control can include cryptographic key management, which is the process of generating, distributing, storing, using, and destroying cryptographic keys in a secure manner. Cryptographic key management is essential for ensuring the security and functionality of cryptographic solutions, such as encryption, digital signatures, or authentication.

The standard provides the following guidance for implementing this control:

A policy on the use of cryptographic controls should be developed and implemented.

The policy should define the circumstances and conditions in which the different types of cryptographic controls should be used, based on the information classification scheme, the relevant agreements, legislation, and regulations, and the assessed risks.

The policy should also define the standards and techniques to be used for each type of cryptographic control, such as the algorithms, key lengths, key formats, and key lifecycles. The policy should be reviewed and updated regularly to reflect the changes in the technology, the business environment, and the legal requirements.

The cryptographic keys should be managed through their whole lifecycle, from generation to destruction, in a secure and controlled manner, following the principles of need-to-know and segregation of duties.

The cryptographic keys should be protected from unauthorized access, disclosure, modification, loss, or theft, using appropriate physical and logical security measures, such as encryption, access control, backup, and audit.

The cryptographic keys should be changed or replaced periodically, or when there is a suspicion of compromise, following a defined process that ensures the continuity of the cryptographic services and the availability of the information.

The cryptographic keys should be securely destroyed when they are no longer required, or when they reach their end of life, using methods that prevent their recovery or reconstruction.

References:

ISO/IEC 27001:2022 Lead Implementer Course Guide¹

ISO/IEC 27001:2022 Lead Implementer Info Kit²

ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 Understanding Cryptographic Controls in Information Security5

NEW QUESTION: 5

Which statement is an example of risk retention?

- A.** An organization has decided to release the software even though some minor bugs have not been fixed yet
- B.** An organization terminates work in the construction site during a severe storm
- C.** An organization has implemented a data loss protection software

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 6

What is an example of a good physical security measure?

- A.** Maintenance staff can be given quick and unimpeded access to the server area in the event of disaster.
- B.** Printers that are defective or have been replaced are immediately removed and given away as garbage for recycling.
- C.** All employees and visitors carry an access pass.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 7

An organization has decided to conduct information security awareness and training sessions on a monthly basis for all employees. Only 45% of employees who attended these sessions were able to pass the exam.

What does the percentage represent?

- A.** Measurement objective
- B.** Attribute
- C.** Performance indicator

Answer: ([SHOW ANSWER](#))

Explanation

According to the ISO/IEC 27001:2022 standard, a performance indicator is "a metric that provides information about the effectiveness or efficiency of an activity, process, system or organization" (section 3.35). A performance indicator should be measurable, relevant, achievable, realistic and time-bound (SMART). In this case, the percentage of employees who passed the exam is a performance indicator that measures the effectiveness of the information security awareness and training sessions. It shows how well the sessions achieved their intended learning outcomes and how well the employees understood the information security concepts and practices.

References:

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection -
Information security management systems - Requirements1 ISO/IEC 27001 Lead
Implementer Info Kit Key performance indicators for an ISO 27001 ISMS2

NEW QUESTION: 8

Prior to employment, _____ as well as terms & conditions of employment are included as controls in ISO

27002 to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

- A. authorizing
- B. screening
- C. flexing
- D. controlling

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 9

Based on scenario 4, the fact that TradeB defined the level of risk based on three nonnumerical categories indicates that;

- A. The level of risk will be evaluated using quantitative analysis
- B. The level of risk will be evaluated against qualitative criteria
- C. The level of risk will be defined using a formula

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 10

A small organization that is implementing an ISMS based on ISO/IEC 27001 has decided to outsource the internal audit function to a third party. Is this acceptable?

- A. No, the organizations cannot outsource the internal audit function to a third party because during internal audit, the organization audits its own system
- B. Yes, outsourcing the internal audit function to a third party is often a better option for small organizations to demonstrate independence and impartiality
- C. No, the outsourcing of the internal audit function may compromise the independence and impartiality of the internal audit team

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 11

An organization that has an ISMS in place conducts management reviews at planned intervals, but does not retain documented information on the results. Is this in accordance with the requirements of ISO/IEC 27001?

- A. No, ISO/IEC 27001 requires organizations to document the results of management reviews

B. Yes. ISO/IEC 27001 does not require organizations to document the results of management reviews

C. Yes. ISO/IEC 27001 requires organizations to document the results of management reviews only if they are conducted ad hoc

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 12

Based on scenario 9. did the ISMS project manager complete the corrective action process appropriately?

A. Yes, the corrective action process should include the identification of the nonconformity, situation analysis, and implementation of corrective actions

B. No, the corrective action process should also include the review of the implementation of the selected actions

C. No, the corrective action did not address the root cause of the nonconformity

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 13

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a combined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit. The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS.

However, the company requested from the certification body that the documentation could not be carried off-site. However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement. The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body. Based on the scenario above, answer the following question:

Does NetworkFuse fulfill the prerequisites for a certification audit?

A. Yes, because the certification body has been selected

B. Yes, because internal audits and management reviews have been performed

C. Yes, because the ISMS must be operational for at least one year prior to the certification audit

Answer: B ([LEAVE A REPLY](#))

Explanation

According to ISO/IEC 27006:2015, the prerequisites for a certification audit are:

The ISMS must be operational for a period of time that is sufficient to demonstrate its effectiveness and performance.

The organization must have conducted at least one internal audit and one management review of the ISMS prior to the certification audit.

The organization must provide the certification body with access to all the relevant documented information, records, personnel, and facilities related to the ISMS.

In the scenario, NetworkFuse has fulfilled these prerequisites, as it has had an operational ISMS for approximately two years, and it has performed internal audits and management reviews. Therefore, the correct answer is B.

References: ISO/IEC 27006:2015, clauses 9.1.1, 9.1.2, and 9.2.1.

NEW QUESTION: 14

According to scenario 7, a demilitarized zone (DMZ) is deployed within InfoSec's network. What type of control has InfoSec implemented in this case?

A. Preventive

B. Detective

C. Corrective

Answer: A (LEAVE A REPLY)

NEW QUESTION: 15

Scenario 4: TradeB, a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001. Having no experience of a management

[^system implementation, TradeB's top management contracted two experts to direct and manage the ISMS implementation project.

First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives. Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category. They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity. Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable

level, the risks will be accepted Based on the scenario above, answer the following question:

The decision to treat only risks that were classified as high indicates that Trade B has:

- A. Evaluated other risk categories based on risk treatment criteria
- B. Modified other risk categories based on risk evaluation criteria
- C. Accepted other risk categories based on risk acceptance criteria

Answer: C (LEAVE A REPLY)

NEW QUESTION: 16

It is allowed that employees and contractors are provided with an anonymous reporting channel to report violations of information security policies or procedures ("whistle blowing")

- A. True
- B. False

Answer: A (LEAVE A REPLY)

Valid ISO-IEC-27001-Lead-Implementer Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Implementer Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Implementer exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Implementer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Implementer dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Implementer_examcollection.html (**350** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 17

Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on ISO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.

Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever Tessa concluded that SunDee

must evaluate the performance of the ISMS adequately. She defined SunDee's negligence of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management Based on the scenario above, answer the following question:

What caused SunDee's workforce disruption?

- A. The voluminous written reports
- B. The negligence of performance evaluation and monitoring and measurement procedures
- C. The inconsistency of reports written by different employees

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 18

Based on scenario 7. InfoSec contracted Anna as an external consultant. Based on her tasks, is this action compliant with ISO/IEC 27001°

- A. Yes, forensic investigation may be conducted internally or by using external consultants
- B. No, the skills of incident response or forensic analysis shall be developed internally
- C. Yes, organizations must use external consultants for forensic investigation, as required by the standard

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 19

What is the best way to comply with legislation and regulations for personal data protection?

- A. Maintaining an incident register
- B. Performing a vulnerability analysis
- C. Performing a threat analysis
- D. Appointing the responsibility to someone

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 20

What is the next step that Operaze's ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.

- A. Obtain top management's approval for the information security policy
- B. Communicate the information security policy to all employees
- C. Implement the information security policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 21

Which of the actions presented in scenario 4 is NOT compliant with the requirements of ISO/IEC 27001?

- A. The external experts selected security controls and drafted the Statement of Applicability
- B. The Statement of Applicability was drafted before conducting the risk assessment
- C. TradeB selected only ISO/IEC 27001 controls deemed applicable to the company

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 22

Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration testing and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties. In addition, the top management of Operaze decided to include most of the company's departments within the ISMS scope. The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties. In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.

Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled. However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.

Operaze decided to migrate its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company. Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.

What is the next step that Operaze's ISMS implementation team should take after drafting the information security policy? Refer to scenario 5.

- A. Implement the information security policy

B. Obtain top management's approval for the information security policy

C. Communicate the information security policy to all employees

Answer: (SHOW ANSWER)

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, the information security policy is a high-level document that defines the organization's objectives, principles, and commitments regarding information security. The policy should be aligned with the organization's strategic direction and context, and should provide a framework for setting information security objectives and establishing the ISMS. The policy should also be approved by top management, who are ultimately responsible for the ISMS and its performance.

Therefore, after drafting the information security policy, the next step that Operaze's ISMS implementation team should take is to obtain top management's approval for the policy.

This will ensure that the policy is consistent with the organization's vision and values, and that it has the necessary support and resources for its implementation and maintenance.

References:

ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 5.2 Policy

ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 12, Information security policy

NEW QUESTION: 23

Diana works as a customer service representative for a large e-commerce company. One day, she accidentally modified the order details of a customer without their permission. Due to this error, the customer received an incorrect product. Which information security principle was breached in this case?

A. Availability

B. Confidentiality

C. Integrity

Answer: C (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001:2022, information security controls are measures that are implemented to protect the confidentiality, integrity, and availability of information assets¹. Controls can be preventive, detective, or corrective, depending on their purpose and nature². Preventive controls aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Detective controls aim to detect or discover the occurrence of a security incident or its symptoms. Corrective controls aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact².

In this scenario, Socket Inc. implemented several security controls to prevent information security incidents from recurring, such as:

Segregation of networks: This is a preventive and technical control that involves separating different parts of a network into smaller segments, using devices such as routers, firewalls, or VPNs, to limit the access and communication between them³. This can enhance the

security and performance of the network, as well as reduce the administrative efforts and costs³.

Privileged access rights: This is a preventive and administrative control that involves granting access to information assets or systems only to authorized personnel who have a legitimate need to access them, based on their roles and responsibilities⁴. This can reduce the risk of unauthorized access, misuse, or modification of information assets or systems⁴.

Cryptographic controls: This is a preventive and technical control that involves the use of cryptography, which is the science of protecting information by transforming it into an unreadable format, to protect the confidentiality, integrity, and authenticity of information assets or systems. This can prevent unauthorized access, modification, or disclosure of information assets or systems.

Information security threat management: This is a preventive and administrative control that involves the identification, analysis, and response to information security threats, which are any incidents that could negatively affect the confidentiality, integrity, or availability of information assets or systems.

This can help the organization to anticipate, prevent, or mitigate the impact of information security threats.

Information security integration into project management: This is a preventive and administrative control that involves the incorporation of information security requirements and controls into the planning, execution, and closure of projects, which are temporary endeavors undertaken to create a unique product, service, or result. This can ensure that information security risks and opportunities are identified and addressed throughout the project life cycle.

However, information backup is not a preventive control, but a corrective control.

Information backup is a corrective and technical control that involves the creation and maintenance of copies of information assets or systems, using dedicated software and utilities, to ensure that they can be recovered in case of data loss, corruption, accidental deletion, or cyber incidents. This can help the organization to restore the normal state of information assets or systems after a security incident or mitigate its impact. Therefore, information backup does not prevent information security incidents from recurring, but rather helps the organization to recover from them.

References:

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection -

Information security management systems - Requirements ISO 27001 Key Terms - PJR

Network Segmentation: What It Is and How It Works | Imperva ISO 27001:2022 Annex A

8.2 - Privileged Access Rights - ISMS.online

[ISO 27001:2022 Annex A 8.3 - Cryptographic Controls - ISMS.online]

[ISO 27001:2022 Annex A 5.30 - Information Security Threat Management - ISMS.online]

[ISO 27001:2022 Annex A 5.31 - Information Security Integration into Project Management - ISMS.online]

[ISO 27001:2022 Annex A 8.13 - Information Backup - ISMS.online]

NEW QUESTION: 24

Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the involved parties, including parents, other physicians, and the medical laboratory staff. Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software. Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.

Which situation described in scenario 1 represents a threat to HealthGenic?

- A. HealthGenic did not train its personnel to use the software
- B. The software company modified information related to HealthGenic's patients
- C. HealthGenic used a web-based medical software for storing patients' confidential information

Answer: B (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001:2022, a threat is any incident that could negatively affect the confidentiality, integrity or availability of an asset¹. In this scenario, the asset is the information related to HealthGenic's patients, which is stored and processed by the web-based medical software. The software company's modification of some files that comprised sensitive information related to HealthGenic's patients is an incident that could negatively affect the confidentiality and integrity of the asset, as it resulted in incomplete and incorrect medical reports and invaded the patients' privacy. Therefore, this situation represents a threat to HealthGenic.

References:

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection - Information security management systems - Requirements ISO 27001 Key Terms - PJR

NEW QUESTION: 25

A non-human threat for computer systems is a flood. In which situation is a flood always a relevant threat?

- A. When the organization is located near a river.
- B. When computer systems are kept in a cellar below ground level.
- C. When the computer systems are not insured.

D. If the riskanalysis has not been carried out.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 26

A company decided to use an algorithm that analyzes various attributes of customer behavior, such as browsing patterns and demographics, and groups customers based on their similar characteristics. This way.

the company will be able to identify frequent buyers and trend-followers, among others.

What type of machine learning this the company using?

A. Decision tree machine learning

B. Supervised machine learning

C. Unsupervised machine learning

Answer: C ([LEAVE A REPLY](#))

Explanation

According to the ISO/IEC 27001 : 2022 Lead Implementer course, one of the objectives of information security incident management is to collect and preserve records that can be used as evidence for disciplinary and legal action, as well as for learning and improvement purposes¹. Therefore, Anna should be aware of the collection and preservation of records when gathering data for the forensics team. She should follow the guidelines and procedures specified in the information security incident management policy of InfoSec, which defines the type, format, content, and location of the records to be created and maintained². The records should be accurate, complete, consistent, and reliable, and should be protected from unauthorized access, modification, or deletion³.

References: 1: PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Information Security Incident Management, slide 16 2: PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Information Security Incident Management, slide 19 3: PECB, ISO/IEC 27001 Lead Implementer Course, Module 8: Information Security Incident Management, slide 20

NEW QUESTION: 27

One of the ways Internet of Things (IoT) devices can communicate with each other (or 'the outside world') is using a so-called short-range radio protocol. Which kind of short-range radio protocol makes it possible to use your phone as a credit card?

A. Near Field Communication (NFC)

B. Bluetooth

C. Radio Frequency Identification (RFID)

D. The 4G protocol

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 28

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.

Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e-commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gained access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

According to scenario 2. Beauty has reviewed all user access rights. What type of control is this?

A. Detective and administrative

B. Corrective and managerial

C. Legal and technical

Answer: ([SHOW ANSWER](#))

Explanation

According to ISO/IEC 27001:2022, controls can be classified into different types based on their nature and purpose¹. Some of the common types of controls are:

Preventive controls: These are controls that aim to prevent or deter the occurrence of a security incident or reduce its likelihood. Examples of preventive controls are encryption, firewalls, locks, policies, etc.

Detective controls: These are controls that aim to detect or discover the occurrence of a security incident or its symptoms. Examples of detective controls are logs, alarms, audits, etc.

Corrective controls: These are controls that aim to correct or restore the normal state of an asset or a process after a security incident or mitigate its impact. Examples of corrective controls are backups, recovery plans, incident response teams, etc.

Administrative controls: These are controls that involve the management and governance of information security, such as policies, procedures, roles, responsibilities, awareness, training, etc.

Technical controls: These are controls that involve the use of technology or software to implement information security, such as encryption, firewalls, anti-malware, authentication, etc.

Physical controls: These are controls that involve the protection of physical assets or locations from unauthorized access, damage, or theft, such as locks, fences, cameras, guards, etc.

Legal controls: These are controls that involve the compliance with laws, regulations, contracts, or agreements related to information security, such as privacy laws, data protection laws, confidentiality agreements, etc.

In this scenario, reviewing all user access rights is a type of detective and administrative control. It is a detective control because it helps to identify any unauthorized or inappropriate access to sensitive information or systems. It is also an administrative control because it involves the definition and enforcement of policies and procedures for granting, revoking, and monitoring user access rights.

References:

ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection -
Information security management systems - Requirements

NEW QUESTION: 29

Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs, computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.

Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security-related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.

One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues. Based on scenario 6, Lisa found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. What does this indicate?

- A.** Lisa did not take actions to acquire the necessary competence
- B.** The effectiveness of the training and awareness session was not evaluated
- C.** Skyver did not determine differing team needs in accordance to the activities they perform and the intended results

Answer: ([SHOW ANSWER](#))

Explanation

According to the ISO/IEC 27001:2022 Lead Implementer Training Course Guide¹, one of the requirements of ISO/IEC 27001 is to ensure that all persons doing work under the organization's control are aware of the information security policy, their contribution to the effectiveness of the ISMS, the implications of not conforming to the ISMS requirements, and the benefits of improved information security performance. To achieve this, the organization should determine the necessary competence of persons doing work under its control that affects its information security performance, provide training or take other actions to acquire the necessary competence, evaluate the effectiveness of the actions taken, and retain appropriate documented information as evidence of competence. The organization should also determine differing team needs in accordance to the activities they perform and the intended results, and provide appropriate training and awareness programs to meet those needs.

Therefore, the scenario indicates that Skyver did not determine differing team needs in accordance to the activities they perform and the intended results, since Lisa, who works in the HR Department, found some of the issues being discussed in the training and awareness session too technical, thus not fully understanding the session. This implies that the session was not tailored to the specific needs and roles of the HR personnel, and that the information security expert did not consider the level of technical knowledge and skills required for them to perform their work effectively and securely.

References:

ISO/IEC 27001:2022 Lead Implementer Training Course Guide¹

ISO/IEC 27001:2022 Lead Implementer Info Kit²

NEW QUESTION: 30

Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs, computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.

Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security-related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.

One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an

honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues Based on the scenario above, answer the following question:

How should Colin have handled the situation with Lisa?

- A.** Deliver training and awareness sessions for employees with the same level of competence needs based on the activities they perform within the company
- B.** Extend the duration of the training and awareness session in order to be able to achieve better results
- C.** Promise Lisa that future training and awareness sessions will be easily understandable

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

The IT Department of a financial institution decided to implement preventive controls to avoid potential security breaches. Therefore, they separated the development, testing, and operating equipment, secured their offices, and used cryptographic keys. However, they are seeking further measures to enhance their security and minimize the risk of security breaches. Which of the following controls would help the IT Department achieve this objective?

- A.** Alarms to detect risks related to heat, smoke, fire, or water
- B.** Change all passwords of all systems
- C.** An access control software to restrict access to sensitive files

Answer: **C** ([LEAVE A REPLY](#))

Explanation

An access control software is a type of preventive control that is designed to limit the access to sensitive files and information based on the user's identity, role, or authorization level. An access control software helps to protect the confidentiality, integrity, and availability of the information by preventing unauthorized users from viewing, modifying, or deleting it. An access control software also helps to create an audit trail that records who accessed what information and when, which can be useful for accountability and compliance purposes.

The IT Department of a financial institution decided to implement preventive controls to avoid potential security breaches. Therefore, they separated the development, testing, and operating equipment, secured their offices, and used cryptographic keys. However, they are seeking further measures to enhance their security and minimize the risk of security breaches. An access control software would help the IT Department achieve this objective by adding another layer of protection to their sensitive files and information, and ensuring that only authorized personnel can access them.

References:

ISO/IEC 27001:2022 Lead Implementer Course Guide1

ISO/IEC 27001:2022 Lead Implementer Info Kit2

ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 What are Information Security Controls? - SecurityScorecard4 What Are the Types of Information Security Controls? - RiskOptics2 Integrity is the property of safeguarding the accuracy and completeness of information and processing methods. A breach of integrity occurs when information is modified or destroyed in an unauthorized or unintended manner. In this case, Diana accidentally modified the order details of a customer without their permission, which resulted in the customer receiving an incorrect product. This means that the information about the customer's order was not accurate or complete, and therefore, the integrity principle was breached. Availability and confidentiality are two other information security principles, but they were not violated in this case. Availability is the property of being accessible and usable upon demand by an authorized entity, and confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems. References: ISO/IEC 27001:2022 Lead Implementer Course Content, Module 5: Introduction to Information Security Controls based on ISO/IEC 27001:20221; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 3.7: Integrity2

Valid ISO-IEC-27001-Lead-Implementer Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Implementer Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Implementer exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Implementer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Implementer dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Implementer_examcollection.html (**350** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 32

What supports the continual improvement of an ISMS?

- A. The update of documented information
- B. The update of external audit reports
- C. The update of action plans

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 33

What is the main purpose of Annex A 7.1 Physical security perimeters of ISO/IEC 27001?

- A. To ensure access to information and other associated assets is defined and authorized
- B. To prevent unauthorized physical access, damage, and interference to the organization's information and other associated assets

C. To maintain the confidentiality of information that is accessible by personnel or external parties

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 34

NetworkFuse should_____to ensure that employees are prepared for the audit. Refer to scenario 10.

A. Conduct practice interviews

B. Observe the technologies used

C. Select a certification body that provides combined audits

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 35

Scenario 6: Skyver offers worldwide shipping of electronic products, including gaming consoles, flat-screen TVs, computers, and printers. In order to ensure information security, the company has decided to implement an information security management system (ISMS) based on the requirements of ISO/IEC 27001.

Colin, the company's best information security expert, decided to hold a training and awareness session for the personnel of the company regarding the information security challenges and other information security-related controls. The session included topics such as Skyver's information security approaches and techniques for mitigating phishing and malware.

One of the participants in the session is Lisa, who works in the HR Department. Although Colin explains the existing Skyver's information security policies and procedures in an honest and fair manner, she finds some of the issues being discussed too technical and does not fully understand the session. Therefore, in a lot of cases, she requests additional help from the trainer and her colleagues What is the difference between training and awareness? Refer to scenario 6.

A. Training helps acquire certain skills, whereas awareness develops certain habits and behaviors.

B. Training helps acquire a skill, whereas awareness helps apply it in practice

C. Training helps transfer a message with the intent of informing, whereas awareness helps change the behavior toward the message

Answer: A ([LEAVE A REPLY](#))

Explanation

According to ISO/IEC 27001, training and awareness are two different but complementary activities that aim to enhance the information security competence and performance of the organization's personnel. Training is the process of providing instruction and guidance to help individuals acquire certain skills, knowledge, or abilities related to information security. Awareness is the process of raising the level of consciousness and understanding of the

importance and benefits of information security, and developing certain habits and behaviors that support the information security objectives and requirements.

In scenario 6, Colin is holding a training and awareness session for the personnel of Skyver, which means he is combining both activities to achieve a more effective and comprehensive information security education. The training part of the session covers topics such as Skyver's information security policies and procedures, and techniques for mitigating phishing and malware. The awareness part of the session covers topics such as Skyver's information security approaches and challenges, and the benefits of information security for the organization and its customers. The purpose of the session is to help the personnel acquire the necessary skills to perform their information security roles and responsibilities, and to develop the appropriate habits and behaviors to protect the information assets of the organization.

References:

ISO/IEC 27001:2013, clause 7.2.2: Information security awareness, education and training
ISO/IEC 27001 Lead Implementer Course, Module 6: Implementing the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 7: Performance evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 8: Continual improvement of the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 9: Preparing for the ISMS certification audit
ISO 27001 Security Awareness Training and Compliance - InfosecTrain
1 ISO/IEC 27001 compliance and cybersecurity awareness training
2 ISO 27001 Free Training | Online Course | British Assessment Bureau

NEW QUESTION: 36

An organization that has an ISMS in place conducts management reviews at planned intervals, but does not retain documented information on the results. Is this in accordance with the requirements of ISO/IEC 27001?

- A.** Yes. ISO/IEC 27001 does not require organizations to document the results of management reviews
- B.** No, ISO/IEC 27001 requires organizations to document the results of management reviews
- C.** Yes. ISO/IEC 27001 requires organizations to document the results of management reviews only if they are conducted ad hoc

Answer: B ([LEAVE A REPLY](#))

Explanation

According to ISO/IEC 27001:2022, clause 9.3.3, the organization must retain documented information as evidence of the results of management reviews. The results of management reviews must include decisions and actions related to the ISMS policy, objectives, risks, opportunities, resources, and communication.

Documenting the results of management reviews is important to ensure the accountability, traceability, and effectiveness of the ISMS. It also helps the organization to monitor and

measure the performance and improvement of the ISMS, and to demonstrate compliance with the requirements of ISO/IEC 27001:2022.

Therefore, an organization that has an ISMS in place and conducts management reviews at planned intervals, but does not retain documented information on the results, is not in accordance with the requirements of ISO/IEC 27001. (From the PECB ISO/IEC 27001

Lead Implementer Course Manual, page 107) References:

PECB ISO/IEC 27001 Lead Implementer Course Manual, page 107

PECB ISO/IEC 27001 Lead Implementer Info Kit, page 7

ISO/IEC 27001:2022 (en), Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clause 9.3.3 1

NEW QUESTION: 37

An organization documented each security control that it Implemented by describing their functions in detail.

Is this compliant with ISO/IEC 27001?

- A.** No, because the documented information should have a strict format, including the date, version number and author identification
- B.** No, the standard requires to document only the operation of processes and controls, so no description of each security control is needed
- C.** Yes, but documenting each security control and not the process in general will make it difficult to review the documented information

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 38

An organization wants to enable the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. Which control should it implement?

- A.** Use of privileged utility programs
- B.** Clock synchronization
- C.** Installation of software on operational systems

Answer: ([SHOW ANSWER](#))

Explanation

Clock synchronization is the control that enables the correlation and analysis of security-related events and other recorded data and to support investigations into information security incidents. According to ISO/IEC

27001:2022, Annex A, control A.8.23.1 states: "The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source." This ensures that the timestamps of the events and data are consistent and accurate across different systems and sources, which facilitates the identification of causal relationships, patterns, trends, and anomalies. Clock

synchronization also helps to establish the sequence of events and the responsibility of the parties involved in an incident.

References:

ISO/IEC 27001:2022, Annex A, control A.8.23.1

PECB ISO/IEC 27001 Lead Implementer Course, Module 7, slide 21

NEW QUESTION: 39

Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB, a document model database that offers high availability, scalability, and flexibility.

Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.

Fortunately, Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions. To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, and regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.

Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Based on scenario 3, what would help Socket Inc. address similar information security incidents in the future?

- A.** Using cryptographic keys to protect the database from unauthorized access
- B.** Using the access control system to ensure that only authorized personnel is granted access
- C.** Using the MongoDB database with the default settings

Answer: B (LEAVE A REPLY)

NEW QUESTION: 40

Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the

[^involved parties, including parents, other physicians, and the medical laboratory staff. Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software. Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.

Based on the scenario above, answer the following question:

Which of the following indicates that the confidentiality of information was compromised?

- A. Service interruptions due to the increased number of users
- B. Invasion of patients' privacy
- C. Modification of patients' medical reports

Answer: B (LEAVE A REPLY)

Explanation

Confidentiality of information is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. In other words, confidentiality ensures that only those who are authorized to access the information can do so. In the scenario, the confidentiality of information was compromised when the software company modified some files that contained sensitive information related to HealthGenic's patients. This modification resulted in the invasion of patients' privacy, which means that their personal and medical information was exposed to unauthorized parties. Therefore, the correct answer is B.

References: : ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements, clause 3.14.

NEW QUESTION: 41

Which statement is an example of risk retention?

- A. An organization has decided to release the software even though some minor bugs have not been fixed yet
- B. An organization has implemented a data loss protection software
- C. An organization terminates work in the construction site during a severe storm

Answer: A (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, risk retention is one of the four risk treatment options that an organization can choose to deal with unacceptable risks. Risk retention means that the organization accepts the risk without taking any action to reduce its likelihood or impact. It applies to risks that are either too costly or impractical to address, or that have a low probability or impact. Therefore, an example of risk retention is when an

organization decides to release the software even though some minor bugs have not been fixed yet. This implies that the organization has assessed the risk of releasing the software with bugs and has determined that it is acceptable, either because the bugs are not critical or because the cost of fixing them would outweigh the benefits.

References:

ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process

3, ISO 27001: Top risk treatment options and controls explained

NEW QUESTION: 42

An organization has implemented a control that enables the company to manage storage media through their life cycle of use. acquisition, transportation and disposal. Which control category does this control belong to?

- A. Technological
- B. Organizational
- C. Physical

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 43

Based on scenario 7, what should Anna be aware of when gathering data?

- A. The collection and preservation of records
- B. The type of data that helps prevent future occurrences of information security incidents
- C. The use of the buffer zone that blocks potential attacks coming from malicious websites where data can be collected

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff. Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information

related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy.

Intrinsic vulnerabilities, such as the _____ are related to the characteristics of the asset. Refer to scenario 1.

- A. Software malfunction
- B. Service interruptions
- C. Complicated user interface

Answer: C (LEAVE A REPLY)

Explanation

Intrinsic vulnerabilities are related to the characteristics of the asset that make it susceptible to threats, regardless of the presence or absence of controls. In scenario 1, the complicated user interface of the web-based medical software is an intrinsic vulnerability, as it is a feature of the software that makes it difficult to use and increases the likelihood of human errors. The software malfunction and the service interruptions are not intrinsic vulnerabilities, but rather incidents that occurred due to external factors, such as the increased number of users or the software company's actions.

References: ISO/IEC 27001:2022 Lead Implementer Course Content, Module 6: Risk Assessment and Treatment¹; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 6.1.2:

Information security risk assessment²

NEW QUESTION: 45

Based on scenario 5. after migrating to cloud. Operaze's IT team changed the ISMS scope and implemented all the required modifications Is this acceptable?

- A. No, because any change in ISMS scope should be accepted by the management
- B. No, because the company has already defined the ISMS scope
- C. Yes, because the ISMS scope should be changed when there are changes to the external environment

Answer: A (LEAVE A REPLY)

NEW QUESTION: 46

Based on scenario 9. is the action plan for the identified nonconformities sufficient to eliminate the detected nonconformities?

- A. No, because the action plan does not include a timeframe for implementation
- B. Yes, because a separate action plan has been created for the identified nonconformity
- C. No, because the action plan does not address the root cause of the identified nonconformity

Answer: A (LEAVE A REPLY)

Valid ISO-IEC-27001-Lead-Implementer Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Implementer Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Implementer exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Implementer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Implementer dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Implementer_examcollection.html (350 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 47

Physical labels and _____ are two common forms of labeling which are mentioned in ISO 27002.

- A. bridge
- B. teradata
- C. metadata

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 48

Who should be involved, among others, in the draft, review, and validation of information security procedures?

- A. The information security committee
- B. The employees in charge of ISMS operation
- C. An external expert

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 49

Scenario 8: SunDee is an American biopharmaceutical company, headquartered in California, the US. It specializes in developing novel human therapeutics, with a focus on cardiovascular diseases, oncology, bone health, and inflammation. The company has had an information security management system (ISMS) based on ISO/IEC 27001 in place for the past two years. However, it has not monitored or measured the performance and effectiveness of its ISMS and conducted management reviews regularly. Just before the recertification audit, the company decided to conduct an internal audit. It also asked most of their staff to compile the written individual reports of the past two years for their departments. This left the Production Department with less than the optimum workforce, which decreased the company's stock.

Tessa was SunDee's internal auditor. With multiple reports written by 50 different employees, the internal audit process took much longer than planned, was very inconsistent, and had no qualitative measures whatsoever. Tessa concluded that SunDee must evaluate the performance of the ISMS adequately. She defined SunDee's negligence

of ISMS performance evaluation as a major nonconformity, so she wrote a nonconformity report including the description of the nonconformity, the audit findings, and recommendations. Additionally, Tessa created a new plan which would enable SunDee to resolve these issues and presented it to the top management Based on scenario 8. does SunDee comply with ISO/IEC 27001 requirements regarding the monitoring and measurement process?

A. Yes. because the standard does not Indicate when the monitoring and measurement phase should be performed

B. Yes, because the standard requires that the monitoring and measurement phase be conducted every two years

C. No, because even though the standard does not imply when such a process should be performed, the company must have a monitoring and measurement process in place

Answer: C (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001:2022, clause 9.1, the organization shall determine: what needs to be monitored and measured, including information security processes and controls, as well as information security performance and the effectiveness of the ISMS; the methods for monitoring, measurement, analysis and evaluation, to ensure valid and reliable results; when the monitoring and measurement shall be performed; who shall monitor and measure; who shall analyze and evaluate the monitoring and measurement results; and how the results shall be communicated and used for decision making and improvement.

The organization shall retain documented information as evidence of the monitoring and measurement results.

The standard does not prescribe a specific frequency or method for monitoring and measurement, but it requires the organization to have a defined and documented process that is appropriate to its context, objectives, risks, and opportunities. The organization should also ensure that the monitoring and measurement results are analyzed and evaluated to determine the performance and effectiveness of the ISMS, and to identify any nonconformities, gaps, or improvement opportunities.

In the scenario, SunDee did not comply with these requirements, as it did not have a monitoring and measurement process in place, and did not monitor or measure the performance and effectiveness of its ISMS regularly. It also did not use valid and reliable methods, or communicate and use the results for improvement.

Therefore, SunDee's negligence of ISMS performance evaluation was a major nonconformity, as Tessa correctly identified.

References: ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection - Information security management systems - Requirements, clause 9.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 9: Monitoring, Measurement, Analysis and Evaluation.

NEW QUESTION: 50

The company Midwest Insurance has taken many measures to protect its information. It uses an Information Security Management System, the input and output of data in applications is validated, confidential documents are sent in encrypted form and staff use tokens to access information systems. Which of these is not a technical measure?

- A. The use of tokens to gain access to information systems
- B. Information Security Management System
- C. Encryption of information
- D. Validation of input and output data in applications

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 51

A company decided to use an algorithm that analyzes various attributes of customer behavior, such as browsing patterns and demographics, and groups customers based on their similar characteristics. This way,

the company will be able to identify frequent buyers and trend-followers, among others.

What type of machine learning is the company using?

- A. Supervised machine learning
- B. Decision tree machine learning
- C. Unsupervised machine learning

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 52

A company moves into a new building. A few weeks after the move, a visitor appears unannounced in the office of the director. An investigation shows that the visitor passes grant the same access as the passes of the company's staff. Which kind of security measure could have prevented this?

- A. An organizational security measure
- B. physical security measure
- C. A technical security measure

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 53

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.

Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e-commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gained access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Based on the scenario above, answer the following question:

After investigating the incident, Beauty decided to install a new anti-malware software.

What type of security control has been implemented in this case?

A. Preventive

B. Detective

C. Corrective

Answer: C ([LEAVE A REPLY](#))

Explanation

A corrective security control is a type of control that is implemented to restore the normal operations of a system or network after a security incident or breach has occurred.

Corrective controls aim to mitigate the impact of the incident, prevent further damage, and restore the confidentiality, integrity, and availability of the information and assets affected by the incident. Examples of corrective controls include backup and recovery, disaster recovery plans, incident response teams, and anti-malware software.

In this case, Beauty decided to install a new anti-malware software after investigating the incident that exposed customers' information due to the out-of-date anti-malware software. The new anti-malware software is a corrective control because it is intended to remove the malicious code that compromised the system and prevent similar incidents from happening again. The new anti-malware software also helps to restore the trust and confidence of the customers and the reputation of the company.

References:

ISO/IEC 27001:2022 Lead Implementer Course Guide1

ISO/IEC 27001:2022 Lead Implementer Info Kit2

ISO/IEC 27001:2022 Information Security Management Systems - Requirements3 ISO/IEC 27002:2022 Code of Practice for Information Security Controls4 What are Security Controls? | IBM3 What Are Security Controls? - F54

NEW QUESTION: 54

Based on scenario 8. did the nonconformity report include all the necessary aspects?

- A. Yes, the report included all the necessary aspects
- B. No, the report must also specify the root cause of the nonconformity
- C. No, the report must also specify the audit criteria

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 55

Which approach should organizations use to implement an ISMS based on ISO/IEC 27001?

- A. Any approach that enables the ISMS implementation within the 12month period
- B. An approach that is suitable for organization's scope
- C. Only the approach provided by the standard

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 56

Who is authorized to change the classification of a document?

- A. The author of the document
- B. The owner of the document
- C. The administrator of the document
- D. The manager of the owner of the document

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 57

Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties In addition, the top management of Operaze decided to Include most of the company's departments within the ISMS scope. The defined scope

included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties. In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.

Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled. However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.

Operaze decided to migrate its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company. Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.

Based on scenario 5, in which category of the interested parties does the HR manager of Operaze belong?

A. Positively influenced interested parties, because the ISMS will increase the effectiveness and efficiency of the HR Department

B. Negatively influenced interested parties, because the HR Department will deal with more documentation

C. Both A and B

Answer: B (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001, interested parties are those who can affect, be affected by, or perceive themselves to be affected by the organization's information security activities, products, or services. Interested parties can be classified into four categories based on their influence and interest in the ISMS:

Positively influenced interested parties: those who benefit from the ISMS and support its implementation and operation

Negatively influenced interested parties: those who are adversely affected by the ISMS and oppose its implementation and operation

High-interest interested parties: those who have a strong interest in the ISMS and its outcomes, regardless of their influence

Low-interest interested parties: those who have a weak interest in the ISMS and its outcomes, regardless of their influence

In scenario 5, the HR manager of Operaze belongs to the category of negatively influenced interested parties, because he/she perceives that the ISMS will create more paperwork and documentation for the HR Department, and therefore opposes its implementation and operation. The HR manager does not benefit from the ISMS and does not support its objectives and requirements.

References:

ISO/IEC 27001:2013, clause 4.2: Understanding the needs and expectations of interested parties
ISO/IEC 27001:2013, Annex A.18.1.4: Assessment of and decision on information security events
ISO/IEC 27001 Lead Implementer Course, Module 2: Introduction to Information Security Management System (ISMS) concepts as required by ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 4: Planning the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 6: Implementing the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 7: Performance evaluation, monitoring and measurement of the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 8: Continual improvement of the ISMS based on ISO/IEC 27001
ISO/IEC 27001 Lead Implementer Course, Module 9: Preparing for the ISMS certification audit

NEW QUESTION: 58

Scenario 1: HealthGenic is a pediatric clinic that monitors the health and growth of individuals from infancy to early adulthood using a web-based medical software. The software is also used to schedule appointments, create customized medical reports, store patients' data and medical history, and communicate with all the [^involved parties, including parents, other physicians, and the medical laboratory staff. Last month, HealthGenic experienced a number of service interruptions due to the increased number of users accessing the software. Another issue the company faced while using the software was the complicated user interface, which the untrained personnel found challenging to use.

The top management of HealthGenic immediately informed the company that had developed the software about the issue. The software company fixed the issue; however, in the process of doing so, it modified some files that comprised sensitive information related to HealthGenic's patients. The modifications that were made resulted in incomplete and incorrect medical reports and, more importantly, invaded the patients' privacy. Based on scenario 1. what is a potential impact of the loss of integrity of information in HealthGenic?

- A.** Disruption of operations and performance degradation
- B.** Incomplete and incorrect medical reports
- C.** Service interruptions and complicated user interface

Answer: B (LEAVE A REPLY)

Explanation

The loss of integrity of information in HealthGenic means that the information was modified or corrupted in an unauthorized or improper way, resulting in inaccurate, incomplete, or unreliable data. This can have a serious impact on the quality and safety of the medical services provided by HealthGenic, as well as the trust and satisfaction of the patients and their families. In particular, incomplete and incorrect medical reports can lead to: Misdiagnosis or delayed diagnosis of the patients' conditions, which can affect their treatment and recovery.

Prescription of wrong or inappropriate medications or dosages, which can cause adverse effects or interactions.

Violation of the patients' privacy and confidentiality, which can expose them to identity theft, fraud, or discrimination.

Legal liability and reputational damage for HealthGenic, which can result in lawsuits, fines, or loss of customers.

Therefore, it is essential for HealthGenic to ensure the integrity of its information by implementing appropriate security controls and measures, such as encryption, authentication, backup, audit, and incident response.

References:

ISO/IEC 27001:2022 Lead Implementer Course Guide¹

ISO/IEC 27001:2022 Lead Implementer Info Kit²

ISO/IEC 27001:2022 Information Security Management Systems - Requirements³ ISO/IEC

27002:2022 Code of Practice for Information Security Controls⁴

NEW QUESTION: 59

Scenario 10: NetworkFuse develops, manufactures, and sells network hardware. The company has had an operational information security management system (ISMS) based on ISO/IEC 27001 requirements and a quality management system (QMS) based on ISO 9001 for approximately two years. Recently, it has applied for a combined certification audit in order to obtain certification against ISO/IEC 27001 and ISO 9001.

After selecting the certification body, NetworkFuse prepared the employees for the audit. The company decided to not conduct a self-evaluation before the audit since, according to the top management, it was not necessary. In addition, it ensured the availability of documented information, including internal audit reports and management reviews, technologies in place, and the general operations of the ISMS and the QMS.

However, the company requested from the certification body that the documentation could not be carried off-site. However, the audit was not performed within the scheduled days because NetworkFuse rejected the audit team leader assigned and requested their replacement. The company asserted that the same audit team leader issued a recommendation for certification to its main competitor, which, for the company's top management, was a potential conflict of interest. The request was not accepted by the certification body. NetworkFuse should _____ to ensure that employees are prepared for the audit. Refer to scenario

10.

A. Conduct practice interviews

B. Observe the technologies used

C. Select a certification body that provides combined audits

Answer: A (LEAVE A REPLY)

Explanation

One of the ways to prepare employees for an ISO/IEC 27001 audit is to conduct practice interviews with them.

This can help them to familiarize themselves with the audit process, the types of questions they might be asked, and the evidence they need to provide to demonstrate compliance with the standard. Practice interviews can also help employees to identify any gaps or weaknesses in their knowledge or performance, and to address them before the actual audit. Practice interviews can be conducted by internal auditors, managers, or consultants, and should cover the relevant scope, objectives, and criteria of the audit. (From the PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113) References:

PECB ISO/IEC 27001 Lead Implementer Course Manual, page 113

PECB ISO/IEC 27001 Lead Implementer Info Kit, page 10

5 Step Plan: How to Prepare for an ISO 27001 Certification Audit

NEW QUESTION: 60

You apply for a position in another company and get the job. Along with your contract, you are asked to sign a code of conduct. What is a code of conduct?

- A.** A code of conduct differs from company to company and specifies, among other things, the rules of behavior with regard to the usage of information systems.
- B.** A code of conduct is a standard part of a labor contract.
- C.** A code of conduct specifies how employees are expected to conduct themselves and is the same for all companies.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 61

Scenario 3: Socket Inc is a telecommunications company offering mainly wireless products and services. It uses MongoDB, a document model database that offers high availability, scalability, and flexibility.

Last month, Socket Inc. reported an information security incident. A group of hackers compromised its MongoDB database, because the database administrators did not change its default settings, leaving it without a password and publicly accessible.

Fortunately, Socket Inc. performed regular information backups in their MongoDB database, so no information was lost during the incident. In addition, a syslog server allowed Socket Inc. to centralize all logs in one server. The company found out that no persistent backdoor was placed and that the attack was not initiated from an employee inside the company by reviewing the event logs that record user faults and exceptions. To prevent similar incidents in the future, Socket Inc. decided to use an access control system that grants access to authorized personnel only. The company also implemented a control in order to define and implement rules for the effective use of cryptography, including cryptographic key management, to protect the database from unauthorized access. The implementation was based on all relevant agreements, legislation, and

regulations, and the information classification scheme. To improve security and reduce the administrative efforts, network segregation using VPNs was proposed.

Lastly, Socket Inc. implemented a new system to maintain, collect, and analyze information related to information security threats, and integrate information security into project management.

Based on scenario 3. which information security control of Annex A of ISO/IEC 27001 did Socket Inc.

implement by establishing a new system to maintain, collect, and analyze information related to information security threats?

A. Annex A 5.5 Contact with authorities

B. Annex A 5.7 Threat Intelligence

C. Annex A 5.13 Labeling of information

Answer: B (LEAVE A REPLY)

Explanation

Annex A 5.7 Threat Intelligence is a new control in ISO 27001:2022 that aims to provide the organisation with relevant information regarding the threats and vulnerabilities of its information systems and the potential impacts of information security incidents. By establishing a new system to maintain, collect, and analyze information related to information security threats, Socket Inc. implemented this control and improved its ability to prevent, detect, and respond to information security incidents.

References:

ISO/IEC 27001:2022 Information technology - Security techniques - Information security management systems - Requirements, Annex A 5.7 Threat Intelligence ISO/IEC

27002:2022 Information technology - Security techniques - Information security, cybersecurity and privacy protection controls, Clause 5.7 Threat Intelligence PECB

ISO/IEC 27001:2022 Lead Implementer Course, Module 6: Implementation of Information Security Controls Based on ISO/IEC 27002:2022, Slide 18: A.5.7 Threat Intelligence

Valid ISO-IEC-27001-Lead-Implementer Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Implementer Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Implementer exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Implementer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Implementer dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Implementer_examcollection.html (**350** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)

NEW QUESTION: 62

An organization has implemented a control that enables the company to manage storage media through their life cycle of use, acquisition, transportation and disposal. Which control category does this control belong to?

A. Organizational

B. Physical

C. Technological

Answer: B ([LEAVE A REPLY](#))

Explanation

According to ISO/IEC 27001:2022, the control that enables the organization to manage storage media through their life cycle of use, acquisition, transportation and disposal belongs to the category of physical and environmental security. This category covers the controls that prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities. The specific control objective for this control is A.11.2.7 Secure disposal or reuse of equipment¹, which states that "equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse."² References:

ISO/IEC 27001:2022, Annex A

ISO/IEC 27002:2022, clause 11.2.7

NEW QUESTION: 63

Who should be involved, among others, in the draft, review, and validation of information security procedures?

A. An external expert

B. The information security committee

C. The employees in charge of ISMS operation

Answer: B ([LEAVE A REPLY](#))

Explanation

According to ISO/IEC 27001:2022, clause 7.5.1, the organization shall ensure that the documented information required by the ISMS and by this document is controlled to ensure that it is available and suitable for use, where and when it is needed, and that it is adequately protected. This includes ensuring that the documented information is reviewed and approved for suitability and adequacy. The information security procedures are part of the documented information that supports the operation of the ISMS processes and the implementation of the information security controls. Therefore, they should be drafted, reviewed, and validated by the information security committee, which is the group of people responsible for overseeing the ISMS and ensuring its alignment with the organization's objectives and strategy. The information security committee should include representatives from different functions and levels of the organization, as well as external experts if needed. The information security committee should also ensure that the

information security procedures are communicated to the relevant employees and other interested parties, and that they are periodically reviewed and updated as necessary.

References:

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection -

Information security management systems - Requirements, clauses 5.3, 7.5.1, and 9.3

ISO/IEC 27001:2022 Lead Implementer objectives and content, 4 and 5

NEW QUESTION: 64

Based on scenario 2, which information security principle is the IT team aiming to ensure by establishing a user authentication process that requires user identification and password when accessing sensitive information?

A. Availability

B. Integrity

C. Confidentiality

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 65

What are the data protection principles set out in the GDPR?

A. Purpose limitation, proportionality, availability, data minimisation

B. Target group, proportionality, transparency, data minimisation

C. Purpose limitation, pudicity, transparency, data minimisation

D. Purpose limitation, proportionality, data minimisation, transparency

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 66

Based on scenario 5. which committee should Operaze create to ensure the smooth running of the ISMS?

A. Management committee

B. Information security committee

C. Operational committee

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 67

How many domains does ISO / IEC 27002: 2013 have?

A. 114

B. 140

C. 14

D. 110

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 68

Scenario 2: Beauty is a cosmetics company that has recently switched to an e-commerce model, leaving the traditional retail. The top management has decided to build their own custom platform in-house and outsource the payment process to an external provider operating online payments systems that support online money transfers.

Due to this transformation of the business model, a number of security controls were implemented based on the identified threats and vulnerabilities associated to critical assets. To protect customers' information.

Beauty's employees had to sign a confidentiality agreement. In addition, the company reviewed all user access rights so that only authorized personnel can have access to sensitive files and drafted a new segregation of duties chart.

However, the transition was difficult for the IT team, who had to deal with a security incident not long after transitioning to the e-commerce model. After investigating the incident, the team concluded that due to the out-of-date anti-malware software, an attacker gained access to their files and exposed customers' information, including their names and home addresses.

The IT team decided to stop using the old anti-malware software and install a new one which would automatically remove malicious code in case of similar incidents. The new software was installed in every workstation within the company. After installing the new software, the team updated it with the latest malware definitions and enabled the automatic update feature to keep it up to date at all times. Additionally, they established an authentication process that requires a user identification and password when accessing sensitive information.

In addition, Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information in order to raise awareness on the importance of system and network security.

Which statement below suggests that Beauty has implemented a managerial control that helps avoid the occurrence of incidents? Refer to scenario 2.

A. Beauty's employees signed a confidentiality agreement

B. Beauty conducted a number of information security awareness sessions for the IT team and other employees that have access to confidential information

C. Beauty updated the segregation of duties chart

Answer: B (LEAVE A REPLY)

Explanation

Managerial controls are administrative actions that are designed to prevent or reduce the likelihood of security incidents by influencing human behavior. They include policies, procedures, guidelines, standards, training, and awareness programs. In scenario 2, Beauty has implemented a managerial control by conducting information security awareness sessions for the IT team and other employees that have access to confidential information. These sessions aim to educate the staff on the importance of system and network security, the potential threats and vulnerabilities, and the best practices to follow to avoid the occurrence of incidents. By raising the level of awareness and knowledge of the

employees, Beauty can reduce the human errors and negligence that might compromise the security of the information assets.

References: ISO/IEC 27001:2022 Lead Implementer Course Content, Module 7: Implementation of an ISMS based on ISO/IEC 27001:20221; ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection, Clause 7.2: Competence2; ISO/IEC 27002:2022 Code of practice for information security controls, Clause 7.2.2: Information security awareness, education and training3

NEW QUESTION: 69

Scenario 9: OpenTech provides IT and communications services. It helps data communication enterprises and network operators become multi-service providers During an internal audit, its internal auditor, Tim, has identified nonconformities related to the monitoring procedures He identified and evaluated several system Invulnerabilities.

Tim found out that user IDs for systems and services that process sensitive information have been reused and the access control policy has not been followed After analyzing the root causes of this nonconformity, the ISMS project manager developed a list of possible actions to resolve the nonconformity. Then, the ISMS project manager analyzed the list and selected the activities that would allow the elimination of the root cause and the prevention of a similar situation in the future. These activities were included in an action plan The action plan, approved by the top management, was written as follows:

A new version of the access control policy will be established and new restrictions will be created to ensure that network access is effectively managed and monitored by the Information and Communication Technology (ICT) Department The approved action plan was implemented and all actions described in the plan were documented.

Based on this scenario, answer the following question:

OpenTech has decided to establish a new version of its access control policy. What should the company do when such changes occur?

- A.** Include the changes in the scope
- B.** Identify the change factors to be monitored
- C.** Update the information security objectives

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 70

Scenario 5: Operaze is a small software development company that develops applications for various companies around the world. Recently, the company conducted a risk assessment to assess the information security risks that could arise from operating in a digital landscape. Using different testing methods, including penetration Resting and code review, the company identified some issues in its ICT systems, including improper user permissions, misconfigured security settings, and insecure network configurations. To resolve these issues and enhance information security, Operaze decided to implement an information security management system (ISMS) based on ISO/IEC 27001.

Considering that Operaze is a small company, the entire IT team was involved in the ISMS implementation project. Initially, the company analyzed the business requirements and the internal and external environment, identified its key processes and activities, and identified and analyzed the interested parties. In addition, the top management of Operaze decided to include most of the company's departments within the ISMS scope. The defined scope included the organizational and physical boundaries. The IT team drafted an information security policy and communicated it to all relevant interested parties. In addition, other specific policies were developed to elaborate on security issues and the roles and responsibilities were assigned to all interested parties.

Following that, the HR manager claimed that the paperwork created by ISMS does not justify its value and the implementation of the ISMS should be canceled. However, the top management determined that this claim was invalid and organized an awareness session to explain the benefits of the ISMS to all interested parties.

Operaze decided to migrate its physical servers to their virtual servers on third-party infrastructure. The new cloud computing solution brought additional changes to the company. Operaze's top management, on the other hand, aimed to not only implement an effective ISMS but also ensure the smooth running of the ISMS operations. In this situation, Operaze's top management concluded that the services of external experts were required to implement their information security strategies. The IT team, on the other hand, decided to initiate a change in the ISMS scope and implemented the required modifications to the processes of the company.

Based on scenario 5, which committee should Operaze create to ensure the smooth running of the ISMS?

A. Information security committee

B. Management committee

C. Operational committee

Answer: A (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001:2022, clause 5.1, the top management of an organization is responsible for ensuring the leadership and commitment for the ISMS. However, the top management may delegate some of its responsibilities to an information security committee, which is a group of people who oversee the ISMS and provide guidance and support for its implementation and operation. The information security committee may include representatives from different departments, functions, or levels of the organization, as well as external experts or consultants. The information security committee may have various roles and responsibilities, such as:

Establishing the information security policy and objectives

Approving the risk assessment and risk treatment methodology and criteria
Reviewing and approving the risk assessment and risk treatment results and plans
Monitoring and evaluating the performance and effectiveness of the ISMS
Reviewing and approving the internal and external audit plans and reports
Initiating and approving corrective and

preventive actions Communicating and promoting the ISMS to all interested parties
Ensuring the alignment of the ISMS with the strategic direction and objectives of the organization
Ensuring the availability of resources and competencies for the ISMS
Ensuring the continual improvement of the ISMS
Therefore, in scenario 5, Operaze should create an information security committee to ensure the smooth running of the ISMS, as this committee would provide the necessary leadership, guidance, and support for the ISMS implementation and operation.

References: ISO/IEC 27001:2022, clause 5.1; PECB ISO/IEC 27001 Lead Implementer Course, Module 4, slide 9.

NEW QUESTION: 71

Scenario 4: TradeB. a commercial bank that has just entered the market, accepts deposits from its clients and offers basic financial services and loans for investments. TradeB has decided to implement an information security management system (ISMS) based on ISO/IEC 27001 Having no experience of a management

[^system implementation, TradeB's top management contracted two experts to direct and manage the ISMS implementation project.

First, the project team analyzed the 93 controls of ISO/IEC 27001 Annex A and listed only the security controls deemed applicable to the company and their objectives Based on this analysis, they drafted the Statement of Applicability. Afterward, they conducted a risk assessment, during which they identified assets, such as hardware, software, and networks, as well as threats and vulnerabilities, assessed potential consequences and likelihood, and determined the level of risks based on three nonnumerical categories (low, medium, and high). They evaluated the risks based on the risk evaluation criteria and decided to treat only the high risk category They also decided to focus primarily on the unauthorized use of administrator rights and system interruptions due to several hardware failures by establishing a new version of the access control policy, implementing controls to manage and control user access, and implementing a control for ICT readiness for business continuity Lastly, they drafted a risk assessment report, in which they wrote that if after the implementation of these security controls the level of risk is below the acceptable level, the risks will be accepted What should TradeB do in order to deal with residual risks? Refer to scenario 4.

- A.** TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment
- B.** TradeB should immediately implement new controls to treat all residual risks
- C.** TradeB should accept the residual risks only above the acceptance level

Answer: A (LEAVE A REPLY)

Explanation

According to ISO/IEC 27001 : 2022 Lead Implementer, residual risk is the risk remaining after risk treatment.

Residual risk should be compared with the acceptable level of risk, which is the level of risk that the organization is willing to tolerate. If the residual risk is below the acceptable level of risk, then the risk can be accepted. If the residual risk is above the acceptable level of risk, then additional risk treatment options should be considered. Therefore, TradeB should evaluate, calculate, and document the value of risk reduction following risk treatment, which is the difference between the initial risk and the residual risk. This will help TradeB to determine whether the risk treatment was effective and whether the residual risk is acceptable or not.

References:

ISO/IEC 27001 : 2022 Lead Implementer Study guide and documents, section 8.3.2 Risk treatment
ISO/IEC 27001 : 2022 Lead Implementer Info Kit, page 14, Risk management process

Valid ISO-IEC-27001-Lead-Implementer Dumps shared by Actual4test.com for Helping Passing ISO-IEC-27001-Lead-Implementer Exam! Actual4test.com now offer the **newest ISO-IEC-27001-Lead-Implementer exam dumps**, the Actual4test.com ISO-IEC-27001-Lead-Implementer exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com ISO-IEC-27001-Lead-Implementer dumps with Test Engine here: https://www.actual4test.com/ISO-IEC-27001-Lead-Implementer_examcollection.html (**350** Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)