PECB.ISO-IEC-27005-Risk-Manager.v2026-04-20.q20

Exam Code:	ISO-IEC-27005-Risk-Manager
Exam Name:	PECB Certified ISO/IEC 27005 Risk Manager
Certification Provider:	PECB
Free Question Number:	20
Version:	v2026-04-20
# of views:	121
# of Questions views:	200
https://www.exam-tests.com/ISO-IEC-27005-Risk-Manager-exam/PECB.ISO-IEC-27005-Risk-Manager.v2026-04-20.q20.html	

NEW QUESTION: 1
Scenario 6: Productscape is a market research company headquartered in Brussels, Belgium. It helps organizations understand the needs and expectations of their customers and identify new business opportunities. Productscape's teams have extensive experience in marketing and business strategy and work with some of the best-known organizations in Europe. The industry in which Productscape operates requires effective risk management. Considering that Productscape has access to clients' confidential information, it is responsible for ensuring its security. As such, the company conducts regular risk assessments. The top management appointed Alex as the risk manager, who is responsible for monitoring the risk management process and treating information security risks.
The last risk assessment conducted was focused on information assets. The purpose of this risk assessment was to identify information security risks, understand their level, and take appropriate action to treat them in order to ensure the security of their systems. Alex established a team of three members to perform the risk assessment activities. Each team member was responsible for specific departments included in the risk assessment scope. The risk assessment provided valuable information to identify, understand, and mitigate the risks that Productscape faces. Initially, the team identified potential risks based on the risk identification results. Prior to analyzing the identified risks, the risk acceptance criteria were established. The criteria for accepting the risks were determined based on Productscape's objectives, operations, and technology. The team created various risk scenarios and determined the likelihood of occurrence as "low," "medium," or "high." They decided that if the likelihood of occurrence for a risk scenario is determined as "low," no further action would be taken. On the other hand, if the likelihood of occurrence for a risk scenario is determined as "high" or "medium," additional controls will be implemented. Some information security risk scenarios defined by Productscape's team were as follows:

1. A cyber attacker exploits a security misconfiguration vulnerability of Productscape's website to launch an attack, which, in turn, could make the website unavailable to users.
2. A cyber attacker gains access to confidential information of clients and may threaten to make the information publicly available unless a ransom is paid.
3. An internal employee clicks on a link embedded in an email that redirects them to an unsecured website, installing a malware on the device.
The likelihood of occurrence for the first risk scenario was determined as "medium." One of the main reasons that such a risk could occur was the usage of default accounts and password. Attackers could exploit this vulnerability and launch a brute-force attack. Therefore, Productscape decided to start using an automated "build and deploy" process which would test the software on deploy and minimize the likelihood of such an incident from happening. However, the team made it clear that the implementation of this process would not eliminate the risk completely and that there was still a low possibility for this risk to occur. Productscape documented the remaining risk and decided to monitor it for changes.
The likelihood of occurrence for the second risk scenario was determined as "medium." Productscape decided to contract an IT company that would provide technical assistance and monitor the company's systems and networks in order to prevent such incidents from happening.
The likelihood of occurrence for the third risk scenario was determined as "high." Thus, Productscape decided to include phishing as a topic on their information security training sessions. In addition, Alex reviewed the controls of Annex A of ISO/IEC 27001 in order to determine the necessary controls for treating this risk. Alex decided to implement control A.8.23 Web filtering which would help the company to reduce the risk of accessing unsecure websites. Although security controls were implemented to treat the risk, the level of the residual risk still did not meet the risk acceptance criteria defined in the beginning of the risk assessment process. Since the cost of implementing additional controls was too high for the company, Productscape decided to accept the residual risk. Therefore, risk owners were assigned the responsibility of managing the residual risk.
Based on scenario 6, Alex reviewed the controls of Annex A of ISO/IEC 27001 to determine the necessary controls for treating the risk described in the third risk scenario. According to the guidelines of ISO/IEC 27005, is this acceptable?
A. No, Annex A controls should be used as a control set only if the organization seeks compliance to ISO/IEC 27001
B. No, organizations should define custom controls that accurately reflect the selected information security risk treatment options
C. Yes. organizations should select all controls from a chosen control set that are necessary for treating the risks
Answer: (SHOW ANSWER)
According to ISO/IEC 27005, organizations can use any set of controls to treat identified risks as long as they are appropriate and necessary for managing those risks. Annex A of ISO/IEC 27001 provides a comprehensive set of controls that can be used to mitigate various information security risks. In this scenario, Alex reviewed the controls from Annex A of ISO/IEC 27001 and selected

control A.8.23 (Web filtering) to treat the risk associated with phishing and accessing unsecured websites. This approach aligns with ISO/IEC 27005, which allows selecting relevant controls from any set to effectively manage risks. Therefore, option C is the correct answer.
Reference:
ISO/IEC 27005:2018, Clause 8.6, "Risk Treatment," which allows for selecting controls from a set, such as Annex A of ISO/IEC 27001, to treat risks appropriately.

NEW QUESTION: 2
Scenario 8: Biotide is a pharmaceutical company that produces medication for treating different kinds of diseases. The company was founded in 1997, and since then it has contributed in solving some of the most challenging healthcare issues.
As a pharmaceutical company, Biotide operates in an environment associated with complex risks. As such, the company focuses on risk management strategies that ensure the effective management of risks to develop high-quality medication. With the large amount of sensitive information generated from the company, managing information security risks is certainly an important part of the overall risk management process. Biotide utilizes a publicly available methodology for conducting risk assessment related to information assets. This methodology helps Biotide to perform risk assessment by taking into account its objectives and mission. Following this method, the risk management process is organized into four activity areas, each of them involving a set of activities, as provided below.
1. Activity area 1: The organization determines the criteria against which the effects of a risk occurring can be evaluated. In addition, the impacts of risks are also defined.
2. Activity area 2: The purpose of the second activity area is to create information asset profiles. The organization identifies critical information assets, their owners, as well as the security requirements for those assets. After determining the security requirements, the organization prioritizes them. In addition, the organization identifies the systems that store, transmit, or process information.
3. Activity area 3: The organization identifies the areas of concern which initiates the risk identification process. In addition, the organization analyzes and determines the probability of the occurrence of possible threat scenarios.
4. Activity area 4: The organization identifies and evaluates the risks. In addition, the criteria specified in activity area 1 is reviewed and the consequences of the areas of concerns are evaluated. Lastly, the level of identified risks is determined.
The table below provides an example of how Biotide assesses the risks related to its information assets following this methodology:

Activity area 1	Activity area 2	Activity area 3	Activity area 4
Main impact areas are: • Reputation • Customer confidence • Legal fines There are three possible levels of impact for these areas: • Low • Moderate • High	**Critical asset:** Electronic health records that are tracked to analyze trends during the development of new drugs. During activity area 2, information for the identified critical asset was gathered and the selection of critical assets was documented. **Security requirements:** **Confidentiality:** Only authorized users should have access to the critical information asset. **Integrity**: This asset can be modified only by authorized users. **Availability**: This asset should be available wherever required by authorized users. The most important security feature of this asset is confidentiality.	**Area of concern 1:** Electronic health records can be accessed by unauthorized users that can exploit the vulnerabilities of the network used for the transmission of the information. **Area of concern 2:** Electronic health records that are tracked to analyze trends for developing new drugs can be modified accidentally by authorized users that have access to this system. For both areas of concern, additional threat scenarios can be identified.	For the identified areas of concern, area of concern 1 has a higher probability of occurring. **The consequences to the company (in case of a breach of security requirements) for area of concern 1:** • Financial loss The severity of each consequence based on impact areas should be determined. By determining the score of each impact area, we find the level of the risk.

Based on scenario 8, how should Biotide use the criteria defined in the activity area 1?

A. To evaluate the potential impact of the risk on Biotide's objectives

B. To identify the assets on which information is stored

C. To determine the probability of threat scenarios

Answer: A (LEAVE A REPLY)

According to ISO/IEC 27005, which provides guidelines for information security risk management, the criteria defined in Activity Area 1 are used to establish the foundation for evaluating the effects of a risk event on an organization's objectives. This is the first step in the risk management process, where the organization must identify its risk evaluation criteria, including the impact levels and their corresponding definitions.

In the context of Biotide, Activity Area 1 involves determining the criteria against which the effects of a risk occurring can be evaluated and defining the impacts of those risks. This directly aligns with ISO/IEC 27005 guidance, where the purpose of setting criteria is to ensure that the potential impact of any risk on the organization's objectives, such as reputation, customer confidence, and legal implications, is comprehensively understood and appropriately managed.

Option A, "To evaluate the potential impact of the risk on Biotide's objectives," is correct because it accurately describes the purpose of defining such criteria: to provide a consistent basis for assessing how various risk scenarios might affect the organization's ability to meet its strategic and operational goals.

Options B and C, which focus on identifying assets or determining the probability of threats, are related to later stages in the risk management process (specifically, Activities 2 and 3), where information assets are profiled and potential threat scenarios are analyzed. Therefore, these do not correspond to the initial criteria definition purpose outlined in Activity Area 1.

NEW QUESTION: 3

Scenario 5: Detika is a private cardiology clinic in Pennsylvania, the US. Detika has one of the most advanced healthcare systems for treating heart diseases. The clinic uses sophisticated apparatus that detects heart diseases in early stages. Since 2010, medical information of Detika's patients is stored on the organization's digital systems. Electronic health records (EHR), among others, include patients' diagnosis, treatment plan, and laboratory results.

Storing and accessing patient and other medical data digitally was a huge and a risky step for Detik a. Considering the sensitivity of information stored in their systems, Detika conducts regular risk assessments to ensure that all information security risks are identified and managed. Last month, Detika conducted a risk assessment which was focused on the EHR system. During risk identification, the IT team found out that some employees were not updating the operating systems regularly. This could cause major problems such as a data breach or loss of software compatibility. In addition, the IT team tested the software and detected a flaw in one of the software modules used. Both issues were reported to the top management and they decided to implement appropriate controls for treating the identified risks. They decided to organize training sessions for all employees in order to make them aware of the importance of the system updates. In addition, the manager of the IT Department was appointed as the person responsible for ensuring that the software is regularly tested.

Another risk identified during the risk assessment was the risk of a potential ransomware attack. This risk was defined as low because all their data was backed up daily. The IT team decided to accept the actual risk of ransomware attacks and concluded that additional measures were not required. This decision was documented in the risk treatment plan and communicated to the risk owner. The risk owner approved the risk treatment plan and documented the risk assessment results.

Following that, Detika initiated the implementation of new controls. In addition, one of the employees of the IT Department was assigned the responsibility for monitoring the implementation process and ensure the effectiveness of the security controls. The IT team, on the other hand, was responsible for allocating the resources needed to effectively implement the new controls.

Based on scenario 5, the IT team was responsible for allocating the necessary resources to ensure that the new controls are implemented effectively. Is this acceptable?

A. Yes, the team that is responsible for conducting the risk assessment should ensure that the necessary resources for treating the risk are allocated

B. No, the organization should allocate the necessary resources to ensure the effective implementation of the risk treatment plan

C. No, the necessary resources for treating the risk should be allocated in the beginning of the risk assessment process

Answer: A (LEAVE A REPLY)

According to ISO/IEC 27005, the team responsible for the risk assessment is often tasked with coordinating the resources necessary to treat identified risks effectively. This includes ensuring that the resources required for implementing risk treatment actions, such as financial, technical, and human resources, are available and allocated appropriately. Option B is incorrect because it

is not only the organization that allocates resources, but rather a combined effort involving the risk management team to ensure proper allocation. Option C is incorrect because resources must be managed and allocated continually throughout the risk management process, not just at the beginning.

NEW QUESTION: 4

Scenario 4: In 2017, seeing that millions of people turned to online shopping, Ed and James Cordon founded the online marketplace for footwear called Poshoe. In the past, purchasing pre-owned designer shoes online was not a pleasant experience because of unattractive pictures and an inability to ascertain the products' authenticity. However, after Poshoe's establishment, each product was well advertised and certified as authentic before being offered to clients. This increased the customers' confidence and trust in Poshoe's products and services. Poshoe has approximately four million users and its mission is to dominate the second-hand sneaker market and become a multi-billion dollar company.

Due to the significant increase of daily online buyers, Poshoe's top management decided to adopt a big data analytics tool that could help the company effectively handle, store, and analyze dat a. Before initiating the implementation process, they decided to conduct a risk assessment. Initially, the company identified its assets, threats, and vulnerabilities associated with its information systems. In terms of assets, the company identified the information that was vital to the achievement of the organization's mission and objectives. During this phase, the company also detected a rootkit in their software, through which an attacker could remotely access Poshoe's systems and acquire sensitive data.

The company discovered that the rootkit had been installed by an attacker who had gained administrator access. As a result, the attacker was able to obtain the customers' personal data after they purchased a product from Poshoe. Luckily, the company was able to execute some scans from the target device and gain greater visibility into their software's settings in order to identify the vulnerability of the system.

The company initially used the qualitative risk analysis technique to assess the consequences and the likelihood and to determine the level of risk. The company defined the likelihood of risk as "a few times in two years with the probability of 1 to 3 times per year." Later, it was decided that they would use a quantitative risk analysis methodology since it would provide additional information on this major risk. Lastly, the top management decided to treat the risk immediately as it could expose the company to other issues. In addition, it was communicated to their employees that they should update, secure, and back up Poshoe's software in order to protect customers' personal information and prevent unauthorized access from attackers.

According to scenario 4, Poshoe has identified its assets, vulnerabilities, and threats associated with its information systems. What does the company need in order to start identifying its existing controls?

A. The risk treatment implementation plan and documentation of controls

B. A list of all existing and planned controls

C. A list of incident scenarios with their consequences

Answer: B (LEAVE A REPLY)
To start identifying its existing controls, Poshoe needs a list of all existing and planned controls. This list will provide the necessary baseline to understand what security measures are already in place and what measures are planned to mitigate risks. This helps in determining gaps, evaluating the effectiveness of current controls, and identifying areas requiring improvement. Option A (The risk treatment implementation plan and documentation of controls) is incorrect because it is too specific and assumes a level of completion not indicated in the scenario. Option C (A list of incident scenarios with their consequences) is incorrect as it pertains to the analysis phase of risk management, not the identification of existing controls.

NEW QUESTION: 5
Scenario 3: Printary is an American company that offers digital printing services. Creating cost-effective and creative products, the company has been part of the printing industry for more than 30 years. Three years ago, the company started to operate online, providing greater flexibility for its clients. Through the website, clients could find information about all services offered by Printary and order personalized products. However, operating online increased the risk of cyber threats, consequently, impacting the business functions of the company. Thus, along with the decision of creating an online business, the company focused on managing information security risks. Their risk management program was established based on ISO/IEC 27005 guidelines and industry best practices.
Last year, the company considered the integration of an online payment system on its website in order to provide more flexibility and transparency to customers. Printary analyzed various available solutions and selected Pay0, a payment processing solution that allows any company to easily collect payments on their website. Before making the decision, Printary conducted a risk assessment to identify and analyze information security risks associated with the software. The risk assessment process involved three phases: identification, analysis, and evaluation. During risk identification, the company inspected assets, threats, and vulnerabilities. In addition, to identify the information security risks, Printary used a list of the identified events that could negatively affect the achievement of information security objectives. The risk identification phase highlighted two main threats associated with the online payment system: error in use and data corruption After conducting a gap analysis, the company concluded that the existing security controls were sufficient to mitigate the threat of data corruption. However, the user interface of the payment solution was complicated, which could increase the risk associated with user errors, and, as a result, impact data integrity and confidentiality.
Subsequently, the risk identification results were analyzed. The company conducted risk analysis in order to understand the nature of the identified risks. They decided to use a quantitative risk analysis methodology because it would provide more detailed information. The selected risk analysis methodology was consistent with the risk evaluation criteri a. Firstly, they used a list of potential incident scenarios to assess their potential impact. In addition, the likelihood of incident scenarios was defined and assessed. Finally, the level of risk was defined as low.

In the end, the level of risk was compared to the risk evaluation and acceptance criteria and was prioritized accordingly.
Based on the scenario above, answer the following question:
What type of risk identification approach did Printary use?
A. Asset-based approach
B. Event-based approach
C. Threat-based approach
Answer: (SHOW ANSWER)
An event-based approach to risk identification focuses on identifying events that could negatively affect the achievement of the organization's objectives. In the scenario, Printary used a list of identified events (e.g., errors in use and data corruption) that could negatively impact their information security objectives. This indicates that they considered specific events that might lead to information security incidents, which is characteristic of an event-based approach. Option B is correct because it aligns with the method described in the scenario. Option A (Asset-based approach) focuses on identifying risks based on assets, while Option C (Threat-based approach) focuses on threats rather than specific events, making them both incorrect in this context.

NEW QUESTION: 6
What type of process is risk management?
A. Ongoing, which allows organizations to monitor risk and keep it at an acceptable level
B. Iterative, which is conducted simultaneously with internal audits to ensure the effectiveness of an organization's operations
C. Ongoing, which must be conducted annually and be consistent with the selection of security controls
Answer: A (LEAVE A REPLY)
Risk management is an ongoing process that involves continuous monitoring, assessment, and mitigation of risks to ensure that they remain within acceptable levels. According to ISO/IEC 27005, risk management is not a one-time activity but a continuous cycle that includes risk identification, risk analysis, risk evaluation, and risk treatment. The process must be regularly reviewed and updated to respond to changes in the organization's environment, technological landscape, or operational conditions. Option A correctly identifies risk management as an ongoing process. Options B and C are incorrect; risk management is not limited to being conducted simultaneously with internal audits (B), nor is it required to be conducted annually (C).

NEW QUESTION: 7
Which activity below is NOT included in the information security risk assessment process?
A. Determining the risk identification approach
B. Prioritizing risks for risk treatment
C. Selecting information security risk treatment options
Answer: C (LEAVE A REPLY)

The information security risk assessment process, as outlined in ISO/IEC 27005, typically includes identifying risks, assessing their potential impact, and prioritizing them. However, selecting risk treatment options is not part of the risk assessment process itself; it is part of the subsequent risk treatment phase. Therefore, option C is the correct answer as it is not included in the risk assessment process.

NEW QUESTION: 8
Based on NIST Risk Management Framework, what is the last step of a risk management process?
A. Monitoring security controls
B. Accessing security controls
C. Communicating findings and recommendations
Answer: A (LEAVE A REPLY)
Based on the NIST Risk Management Framework (RMF), the last step of the risk management process is "Monitoring Security Controls." This step involves continuously tracking the effectiveness of the implemented security controls, ensuring they remain effective against identified risks, and adapting them to any changes in the threat landscape. Option A correctly identifies the final step.

NEW QUESTION: 9
Which of the following risk assessment methods provides an information security risk assessment methodology and involves three phases build asset-based threat profiles, identify infrastructure vulnerabilities, and develop security strategy and plans?
A. OCTAVE-S
B. MEHARI
C. TRA
Answer: A (LEAVE A REPLY)
OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small Organizations) is a risk assessment methodology tailored for small organizations. It provides a structured approach for identifying and managing information security risks. The OCTAVE-S method involves three main phases:
Building asset-based threat profiles, where critical assets and their associated threats are identified.
Identifying infrastructure vulnerabilities by assessing the organization's technological infrastructure for weaknesses that could be exploited by threats.
Developing security strategy and plans to address the identified risks and improve the overall security posture.
The OCTAVE-S method aligns with the description provided in the question, making it the correct answer. MEHARI and TRA are other risk assessment methods, but they do not specifically follow the three phases outlined above.

NEW QUESTION: 10
An organization decided to use nonnumerical categories, i.e., low, medium, and high for describing consequence and probability. Which risk analysis methodology is the organization using?
A. Quantitative
B. Semi-quantitative
C. Qualitative
Answer: C (LEAVE A REPLY)
A qualitative risk analysis method uses nonnumerical categories such as low, medium, and high to describe the consequences and probability of risks. This method involves subjective judgment based on expertise, experience, and intuition rather than mathematical calculations. Qualitative methods are often used when it is challenging to obtain accurate numerical data, and they provide a general understanding of risks to prioritize them for further action. Option C is correct because the use of nonnumerical categories aligns with the qualitative risk analysis methodology. Option A (Quantitative) is incorrect as it involves numerical values and statistical methods, while Option B (Semi-quantitative) is a mix of qualitative and quantitative methods, usually involving ranges of numerical values.

NEW QUESTION: 11
After creating a plan for outsourcing to a cloud service provider to store their confidential information in cloud, OrgX decided to not pursue this business strategy since the risk of doing so was high. Which risk treatment option did OrgX use?
A. Risk avoidance
B. Risk sharing
C. Risk modification
Answer: A (LEAVE A REPLY)
OrgX decided not to pursue a business strategy involving outsourcing to a cloud service provider due to the high risk. This decision reflects a "risk avoidance" strategy, where the organization chooses not to engage in an activity that poses unacceptable risks. This aligns with option A.

NEW QUESTION: 12
What should an organization do after it has established the risk communication plan?
A. Change the communication approach and tools
B. Update the information security policy
C. Establish internal and external communication
Answer: (SHOW ANSWER)
Once an organization has established a risk communication plan, it should implement it by establishing both internal and external communication channels to ensure all stakeholders are informed and involved in the risk management process. This step is crucial for maintaining transparency, ensuring clarity, and fostering a collaborative environment where risks are managed effectively. Therefore, option C is the correct answer.

Reference:
ISO/IEC 27005:2018, Clause 7, "Communication and Consultation," which outlines the importance of establishing both internal and external communication mechanisms to ensure effective risk management.

NEW QUESTION: 13
Scenario 1
The risk assessment process was led by Henry, Bontton's risk manager. The first step that Henry took was identifying the company's assets. Afterward, Henry created various potential incident scenarios. One of the main concerns regarding the use of the application was the possibility of being targeted by cyber attackers, as a great number of organizations were experiencing cyberattacks during that time. After analyzing the identified risks, Henry evaluated them and concluded that new controls must be implemented if the company wants to use the application. Among others, he stated that training should be provided to personnel regarding the use of the application and that awareness sessions should be conducted regarding the importance of protecting customers' personal data.
Lastly, Henry communicated the risk assessment results to the top management. They decided that the application will be used only after treating the identified risks.
According to scenario 1, what type of controls did Henry suggest?
A. Technical
B. Managerial
C. Administrative
Answer: (SHOW ANSWER)
In the context of Scenario 1, the controls suggested by Henry, such as training personnel on the use of the application and conducting awareness sessions on protecting customers' personal data, fall under the category of "Administrative" controls. Administrative controls are policies, procedures, guidelines, and training programs designed to manage the human factors of information security. These controls are aimed at reducing the risks associated with human behavior, such as lack of awareness or improper handling of sensitive data, and are distinct from "Technical" controls (like firewalls or encryption) and "Managerial" controls (which include risk management strategies and governance frameworks).
Reference:
ISO/IEC 27005:2018, Annex A, "Controls and Safeguards," which mentions the importance of administrative controls, such as awareness training and the development of policies, to mitigate identified risks.
ISO/IEC 27001:2013, Annex A, Control A.7.2.2, "Information security awareness, education, and training," which directly relates to administrative controls for personnel security.

NEW QUESTION: 14
Scenario 4: In 2017, seeing that millions of people turned to online shopping, Ed and James Cordon founded the online marketplace for footwear called Poshoe. In the past, purchasing pre-

owned designer shoes online was not a pleasant experience because of unattractive pictures and an inability to ascertain the products' authenticity. However, after Poshoe's establishment, each product was well advertised and certified as authentic before being offered to clients. This increased the customers' confidence and trust in Poshoe's products and services. Poshoe has approximately four million users and its mission is to dominate the second-hand sneaker market and become a multi-billion dollar company.

Due to the significant increase of daily online buyers, Poshoe's top management decided to adopt a big data analytics tool that could help the company effectively handle, store, and analyze dat a. Before initiating the implementation process, they decided to conduct a risk assessment. Initially, the company identified its assets, threats, and vulnerabilities associated with its information systems. In terms of assets, the company identified the information that was vital to the achievement of the organization's mission and objectives. During this phase, the company also detected a rootkit in their software, through which an attacker could remotely access Poshoe's systems and acquire sensitive data.

The company discovered that the rootkit had been installed by an attacker who had gained administrator access. As a result, the attacker was able to obtain the customers' personal data after they purchased a product from Poshoe. Luckily, the company was able to execute some scans from the target device and gain greater visibility into their software's settings in order to identify the vulnerability of the system.

The company initially used the qualitative risk analysis technique to assess the consequences and the likelihood and to determine the level of risk. The company defined the likelihood of risk as "a few times in two years with the probability of 1 to 3 times per year." Later, it was decided that they would use a quantitative risk analysis methodology since it would provide additional information on this major risk. Lastly, the top management decided to treat the risk immediately as it could expose the company to other issues. In addition, it was communicated to their employees that they should update, secure, and back up Poshoe's software in order to protect customers' personal information and prevent unauthorized access from attackers.

Based on scenario 4, which scanning tool did Poshoe use to detect the vulnerability in their software?

A. Network-based scanning tool

B. Host-based scanning tool

C. Penetration testing tool

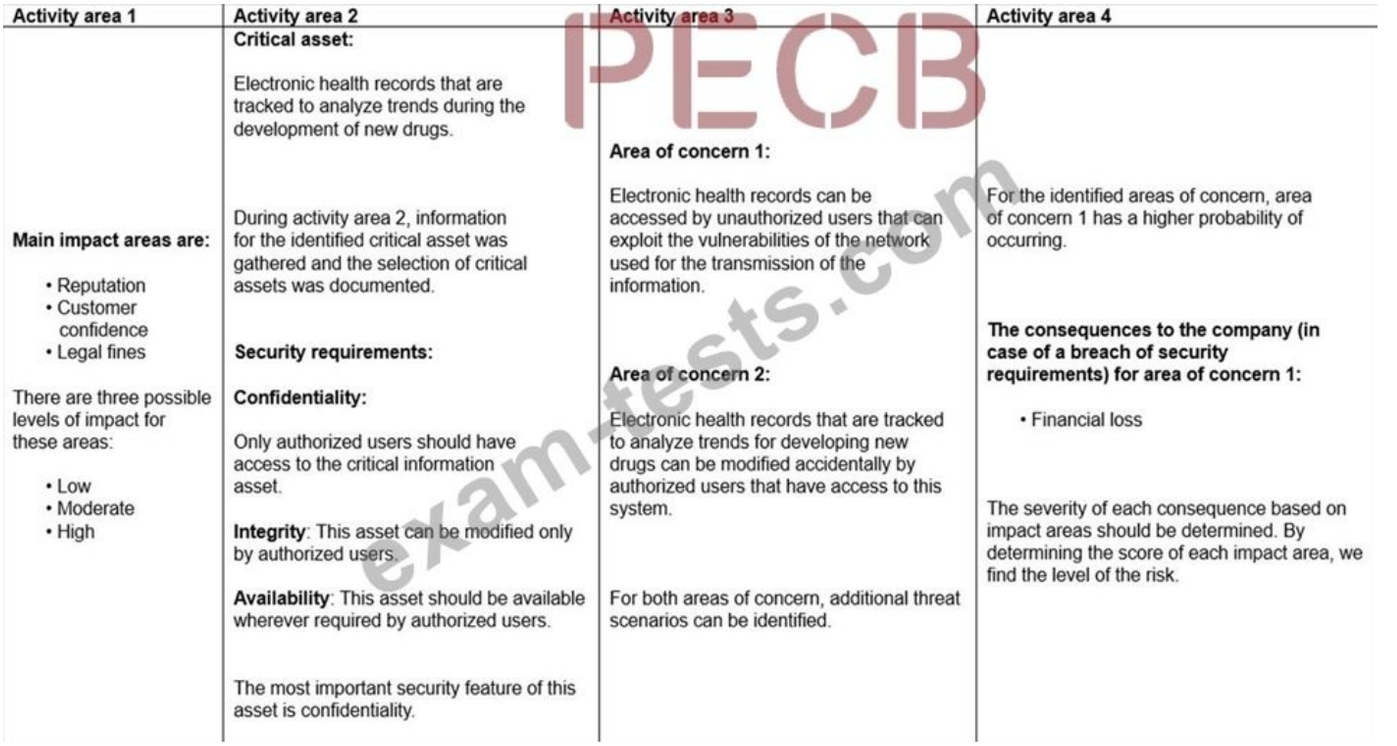
Answer: (SHOW ANSWER)

Poshoe used scans from the target device to gain greater visibility into their software's settings and identify vulnerabilities, which indicates the use of a host-based scanning tool. Host-based scanning tools are used to examine the internal state of a system, such as installed software, configurations, and files, to detect vulnerabilities or malicious software like rootkits. Option A (Network-based scanning tool) would be used to scan network traffic and identify vulnerabilities in network devices, which does not match the context. Option C (Penetration testing tool) involves simulating an attack to test system defenses, which is more intrusive than the scanning described in the scenario.

NEW QUESTION: 15
Scenario 3: Printary is an American company that offers digital printing services. Creating cost-effective and creative products, the company has been part of the printing industry for more than 30 years. Three years ago, the company started to operate online, providing greater flexibility for its clients. Through the website, clients could find information about all services offered by Printary and order personalized products. However, operating online increased the risk of cyber threats, consequently, impacting the business functions of the company. Thus, along with the decision of creating an online business, the company focused on managing information security risks. Their risk management program was established based on ISO/IEC 27005 guidelines and industry best practices.
Last year, the company considered the integration of an online payment system on its website in order to provide more flexibility and transparency to customers. Printary analyzed various available solutions and selected Pay0, a payment processing solution that allows any company to easily collect payments on their website. Before making the decision, Printary conducted a risk assessment to identify and analyze information security risks associated with the software. The risk assessment process involved three phases: identification, analysis, and evaluation. During risk identification, the company inspected assets, threats, and vulnerabilities. In addition, to identify the information security risks, Printary used a list of the identified events that could negatively affect the achievement of information security objectives. The risk identification phase highlighted two main threats associated with the online payment system: error in use and data corruption After conducting a gap analysis, the company concluded that the existing security controls were sufficient to mitigate the threat of data corruption. However, the user interface of the payment solution was complicated, which could increase the risk associated with user errors, and, as a result, impact data integrity and confidentiality.
Subsequently, the risk identification results were analyzed. The company conducted risk analysis in order to understand the nature of the identified risks. They decided to use a quantitative risk analysis methodology because it would provide more detailed information. The selected risk analysis methodology was consistent with the risk evaluation criteri a. Firstly, they used a list of potential incident scenarios to assess their potential impact. In addition, the likelihood of incident scenarios was defined and assessed. Finally, the level of risk was defined as low.
In the end, the level of risk was compared to the risk evaluation and acceptance criteria and was prioritized accordingly.
Did Primary perform risk analysis in accordance with the guidelines of ISO/IEC 27005? Refer to scenario 3.
A. No, the gap analysis should have been conducted during risk analysis, as suggested by ISO/IEC 27005
B. No. according to ISO/IEC 27005, the risk level should be determined during risk evaluation
C. Yes, according to ISO/IEC 27005. the consequences, likelihood, and the level of risk should be determined during risk analysis
Answer: C (LEAVE A REPLY)

ISO/IEC 27005 specifies that risk analysis should involve determining the potential consequences (impact) and the likelihood of identified risks, which together form the basis for calculating the level of risk. In Scenario 3, Printary followed this approach by assessing potential incident scenarios, determining their impact, evaluating their likelihood, and finally defining the level of risk. This process is aligned with the guidelines of ISO/IEC 27005 for conducting a thorough risk analysis. Therefore, Printary performed the risk analysis in accordance with the standard's guidelines, making option C the correct answer.
Reference:
ISO/IEC 27005:2018, Clause 8.4, "Risk Analysis," which outlines the steps to analyze risks by determining their consequences, likelihood, and overall level of risk.

NEW QUESTION: 16
Scenario 8: Biotide is a pharmaceutical company that produces medication for treating different kinds of diseases. The company was founded in 1997, and since then it has contributed in solving some of the most challenging healthcare issues.
As a pharmaceutical company, Biotide operates in an environment associated with complex risks. As such, the company focuses on risk management strategies that ensure the effective management of risks to develop high-quality medication. With the large amount of sensitive information generated from the company, managing information security risks is certainly an important part of the overall risk management process. Biotide utilizes a publicly available methodology for conducting risk assessment related to information assets. This methodology helps Biotide to perform risk assessment by taking into account its objectives and mission. Following this method, the risk management process is organized into four activity areas, each of them involving a set of activities, as provided below.
1. Activity area 1: The organization determines the criteria against which the effects of a risk occurring can be evaluated. In addition, the impacts of risks are also defined.
2. Activity area 2: The purpose of the second activity area is to create information asset profiles. The organization identifies critical information assets, their owners, as well as the security requirements for those assets. After determining the security requirements, the organization prioritizes them. In addition, the organization identifies the systems that store, transmit, or process information.
3. Activity area 3: The organization identifies the areas of concern which initiates the risk identification process. In addition, the organization analyzes and determines the probability of the occurrence of possible threat scenarios.
4. Activity area 4: The organization identifies and evaluates the risks. In addition, the criteria specified in activity area 1 is reviewed and the consequences of the areas of concerns are evaluated. Lastly, the level of identified risks is determined.
The table below provides an example of how Biotide assesses the risks related to its information assets following this methodology:



Activity area 1	Activity area 2	Activity area 3	Activity area 4
Main impact areas are: • Reputation • Customer confidence • Legal fines There are three possible levels of impact for these areas: • Low • Moderate • High	**Critical asset:** Electronic health records that are tracked to analyze trends during the development of new drugs. During activity area 2, information for the identified critical asset was gathered and the selection of critical assets was documented. **Security requirements:** **Confidentiality:** Only authorized users should have access to the critical information asset. **Integrity**: This asset can be modified only by authorized users. **Availability**: This asset should be available wherever required by authorized users. The most important security feature of this asset is confidentiality.	**Area of concern 1:** Electronic health records can be accessed by unauthorized users that can exploit the vulnerabilities of the network used for the transmission of the information. **Area of concern 2:** Electronic health records that are tracked to analyze trends for developing new drugs can be modified accidentally by authorized users that have access to this system. For both areas of concern, additional threat scenarios can be identified.	For the identified areas of concern, area of concern 1 has a higher probability of occurring. **The consequences to the company (in case of a breach of security requirements) for area of concern 1:** • Financial loss The severity of each consequence based on impact areas should be determined. By determining the score of each impact area, we find the level of the risk.

According to the risk assessment methodology used by Biotide, what else should be performed during activity area 4? Refer to scenario 8.

A. Create a strategic and operational plan

B. Select a mitigation strategy for the identified risk profiles

C. Monitor security controls for ensuring they are appropriate for new threats

Answer: B (LEAVE A REPLY)

In Activity Area 4 of the risk assessment methodology used by Biotide, the focus is on identifying and evaluating risks, reviewing the criteria defined in Activity Area 1, and evaluating the consequences of identified areas of concern to determine the level of risk. However, an essential part of completing a risk assessment process also includes determining appropriate mitigation strategies for the identified risks.

ISO/IEC 27005 provides guidance on selecting and implementing security measures to manage the risk to an acceptable level. Therefore, selecting a mitigation strategy for the identified risk profiles is a crucial next step. This involves deciding on controls or measures that will reduce either the likelihood of the threat exploiting the vulnerability or the impact of the risk should it occur. Thus, the correct answer is B.

Reference:

ISO/IEC 27005:2018, Section 8.3.5 "Risk treatment" outlines the process of selecting appropriate risk treatment options (mitigation strategies) once risks have been identified and evaluated.

NEW QUESTION: 17

Scenario 7: Adstry is a business growth agency that specializes in digital marketing strategies. Adstry helps organizations redefine the relationships with their customers through innovative solutions. Adstry is headquartered in San Francisco and recently opened two new offices in New York. The structure of the company is organized into teams which are led by project managers. The project manager has the full power in any decision related to projects. The team members, on the other hand, report the project's progress to project managers.

Considering that data breaches and ad fraud are common threats in the current business environment, managing risks is essential for Adstry. When planning new projects, each project manager is responsible for ensuring that risks related to a particular project have been identified, assessed, and mitigated. This means that project managers have also the role of the risk manager in Adstry. Taking into account that Adstry heavily relies on technology to complete their projects, their risk assessment certainly involves identification of risks associated with the use of information technology. At the earliest stages of each project, the project manager communicates the risk assessment results to its team members.

Adstry uses a risk management software which helps the project team to detect new potential risks during each phase of the project. This way, team members are informed in a timely manner for the new potential risks and are able to respond to them accordingly. The project managers are responsible for ensuring that the information provided to the team members is communicated using an appropriate language so it can be understood by all of them.

In addition, the project manager may include external interested parties affected by the project in the risk communication. If the project manager decides to include interested parties, the risk communication is thoroughly prepared. The project manager firstly identifies the interested parties that should be informed and takes into account their concerns and possible conflicts that may arise due to risk communication. The risks are communicated to the identified interested parties while taking into consideration the confidentiality of Adstry's information and determining the level of detail that should be included in the risk communication. The project managers use the same risk management software for risk communication with external interested parties since it provides a consistent view of risks. For each project, the project manager arranges regular meetings with relevant interested parties of the project, they discuss the detected risks, their prioritization, and determine appropriate treatment solutions. The information taken from the risk management software and the results of these meetings are documented and are used for decision-making processes. In addition, the company uses a computerized documented information management system for the acquisition, classification, storage, and archiving of its documents.

Based on scenario 7, the risk management software is used to help Adstry's teams to detect new risks throughout all phases of the project. Is this necessary?
A. Yes, Adstry; should establish adequate procedures to monitor and review risks on a regular basis in order to identity the changes at an early stage
B. Yes, according to ISO/IEC 27005, Adstry; must use an automated solution for identifying and analyzing risks related to information technology throughout all phases of a project
C. No. monitoring risks after a project is initiated will not provide important information that could impact Adstry'.s business objectives
Answer: A (LEAVE A REPLY)
According to ISO/IEC 27005, it is essential to establish procedures for the continuous monitoring and review of risks to identify changes in the risk environment at an early stage. This ongoing monitoring process helps ensure that new risks are detected promptly and that existing controls remain effective. Option B is incorrect because while automation can aid in risk management, ISO/IEC 27005 does not mandate the use of automated solutions specifically. Option C is incorrect because monitoring risks after a project is initiated is crucial for adapting to changing conditions and protecting business objectives.

NEW QUESTION: 18
Scenario 5: Detika is a private cardiology clinic in Pennsylvania, the US. Detika has one of the most advanced healthcare systems for treating heart diseases. The clinic uses sophisticated apparatus that detects heart diseases in early stages. Since 2010, medical information of Detika's patients is stored on the organization's digital systems. Electronic health records (EHR), among others, include patients' diagnosis, treatment plan, and laboratory results.
Storing and accessing patient and other medical data digitally was a huge and a risky step for Detik a. Considering the sensitivity of information stored in their systems, Detika conducts regular risk assessments to ensure that all information security risks are identified and managed. Last month, Detika conducted a risk assessment which was focused on the EHR system. During risk identification, the IT team found out that some employees were not updating the operating systems regularly. This could cause major problems such as a data breach or loss of software compatibility. In addition, the IT team tested the software and detected a flaw in one of the software modules used. Both issues were reported to the top management and they decided to implement appropriate controls for treating the identified risks. They decided to organize training sessions for all employees in order to make them aware of the importance of the system updates. In addition, the manager of the IT Department was appointed as the person responsible for ensuring that the software is regularly tested.
Another risk identified during the risk assessment was the risk of a potential ransomware attack. This risk was defined as low because all their data was backed up daily. The IT team decided to accept the actual risk of ransomware attacks and concluded that additional measures were not required. This decision was documented in the risk treatment plan and communicated to the risk owner. The risk owner approved the risk treatment plan and documented the risk assessment results.

Following that, Detika initiated the implementation of new controls. In addition, one of the employees of the IT Department was assigned the responsibility for monitoring the implementation process and ensure the effectiveness of the security controls. The IT team, on the other hand, was responsible for allocating the resources needed to effectively implement the new controls.

Based on scenario 5, the decision to accept the risk of a potential ransomware attack was approved by the risk owner. Is this acceptable?

A. No, all interested parties should approve the risk treatment plan

B. No, the risk treatment plan should be approved by the top management and implemented by risk owners

C. Yes, the risk treatment plan should be approved by the risk owners

Answer: C (LEAVE A REPLY)

According to ISO/IEC 27005, the risk treatment plan should be approved by the risk owners, who are the individuals or entities responsible for managing specific risks. In the scenario, the risk owner approved the decision to accept the risk of a potential ransomware attack and documented it in the risk treatment plan. This is consistent with the guidelines, which state that risk owners are responsible for deciding on risk treatment and approving the associated plans. Thus, option C is the correct answer.

Reference:

ISO/IEC 27005:2018, Clause 8.6, "Risk Treatment," which emphasizes that risk treatment plans should be approved by the risk owners.

NEW QUESTION: 19

Which of the following statements best defines information security risk?

A. The potential that threats will exploit vulnerabilities of an information asset and cause harm to an organization

B. Weakness of an asset or control that can be exploited by one or a group of threats

C. Potential cause of an unwanted incident related to information security that can cause harm to an organization

Answer: A (LEAVE A REPLY)

Information security risk, as defined by ISO/IEC 27005, is "the potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization." This definition emphasizes the interplay between threats (e.g., cyber attackers, natural disasters), vulnerabilities (e.g., weaknesses in software, inadequate security controls), and the potential impact or harm that could result from this exploitation. Therefore, option A is the most comprehensive and accurate description of information security risk. In contrast, option B describes a vulnerability, and option C focuses on the cause of an incident rather than defining risk itself. Option A aligns directly with the risk definition in ISO/IEC 27005.

NEW QUESTION: 20

An organization has installed security cameras and alarm systems. What type of information security control has been implemented in this case?

A. Technical

B. Managerial

C. Legal

Answer: A (LEAVE A REPLY)

Security cameras and alarm systems are considered technical controls in the context of information security. Technical controls, also known as logical controls, involve the use of technology to protect information and information systems. These controls are designed to prevent or detect security breaches and mitigate risks related to physical access and surveillance. While security cameras and alarms are physical in nature, they fall under the broader category of technical controls because they involve electronic monitoring and alert systems. Option B (Managerial) refers to administrative policies and procedures, and option C (Legal) refers to controls related to compliance with laws and regulations, neither of which applies in this case.