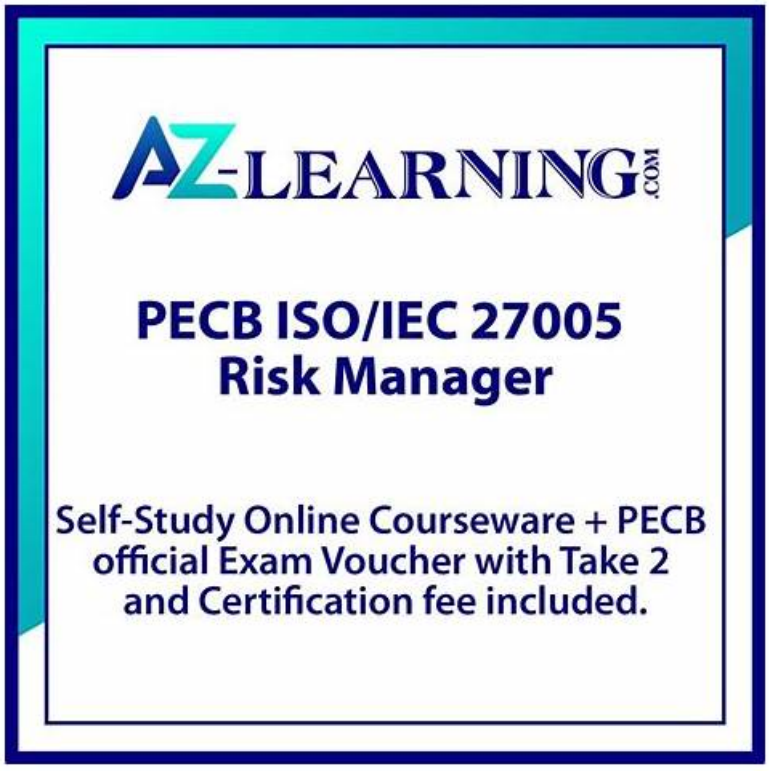
ISO-IEC-27005-Risk-Manager Study Group, Latest Braindumps ISO-IEC-27005-Risk-Manager Book



DOWNLOAD the newest ExamTorrent ISO-IEC-27005-Risk-Manager PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1ceGUZDrmbwAbiOptRbWTMUg-1Woy4Pp9

In life we mustn't always ask others to give me something, but should think what I can do for others. At work if you can create a lot of value for the boss, the boss of course care about your job, including your salary. The same reason, if we are always a ordinary IT staff, yhen you will be eliminated sooner or later. We should pass the IT exams, and go to the top step by step. ExamTorrent's PECB ISO-IEC-27005-Risk-Manager Exam Materials can help you to find shortcut to success. There are a lot of IT people who have started to act. Success is in the ExamTorrent PECB ISO-IEC-27005-Risk-Manager exam training materials. Of course you can not miss it.

ExamTorrent PECB Certified ISO/IEC 27005 Risk Manager (ISO-IEC-27005-Risk-Manager) exam questions are consistently updated to make sure they are according to the PECB latest exam syllabus. If you choose ExamTorrent, you can be sure that you'll always get the updated and real ISO-IEC-27005-Risk-Manager exam questions, which are essential to go through the ISO-IEC-27005-Risk-Manager test in one go. In addition, we also offer up to 1 year of free PECB ISO-IEC-27005-Risk-Manager certification exam question updates. These free updates ensure that candidates get access to the latest PECB exam questions even after they have made their initial purchase.

>> ISO-IEC-27005-Risk-Manager Study Group <<

Pass Guaranteed Quiz ISO-IEC-27005-Risk-Manager - PECB Certified ISO/IEC 27005 Risk Manager Latest Study Group

A good ISO-IEC-27005-Risk-Manager certification must be supported by a good ISO-IEC-27005-Risk-Manager exam practice, which will greatly improve your learning ability and effectiveness. Our study materials have the advantage of short time, high speed and high pass rate. You only take 20 to 30 hours to practice our ISO-IEC-27005-Risk-Manager Guide materials and then you can take the exam. If you use our study materials, you can get the ISO-IEC-27005-Risk-Manager certification by spending very little time and energy reviewing and preparing.

PECB ISO-IEC-27005-Risk-Manager Exam Syllabus Topics:

Topic	Details
Topic 1	• Information Security Risk Management Framework and Processes Based on ISO • IEC 27005: Centered around ISO • IEC 27005, this domain provides structured guidelines for managing information security risks, promoting a systematic and standardized approach aligned with international practices.
Topic 2	• Other Information Security Risk Assessment Methods: Beyond ISO • IEC 27005, this domain reviews alternative methods for assessing and managing risks, allowing organizations to select tools and frameworks that align best with their specific requirements and risk profile.
Topic 3	• Fundamental Principles and Concepts of Information Security Risk Management: This domain covers the essential ideas and core elements behind managing risks in information security, with a focus on identifying and mitigating potential threats to protect valuable data and IT resources.
Topic 4	• Implementation of an Information Security Risk Management Program: This domain discusses the steps for setting up and operationalizing a risk management program, including procedures to recognize, evaluate, and reduce security risks within an organization's framework.

PECB Certified ISO/IEC 27005 Risk Manager Sample Questions (Q25-Q30):

NEW QUESTION # 25
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, organizations should define custom controls that accurately reflect the selected information security risk treatment options
- B. Yes. organizations should select all controls from a chosen control set that are necessary for treating the risks
- C. No, Annex A controls should be used as a control set only if the organization seeks compliance to ISO/IEC 27001

Answer: B

Explanation:
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 # 26
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:
Based on the scenario above, answer the following question:

Activity area 1	Activity area 2	Activity area 3	Activity area 4
	Critical asset: Electronic health records that are tracked to analyze trends during the development of new drugs.		
Main impact areas are: • Reputation • Customer confidence • Legal fines There are three possible levels of impact for these areas: • Low • Moderate • High	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.

Which risk assessment methodology does Biotide use?

- A. MEHARI
- B. OCTAVE Allegro
- C. OCTAVE-S

Answer: B

Explanation:
Biotide uses the OCTAVE Allegro methodology for risk assessment. This is determined based on the description of the activities mentioned in the scenario. OCTAVE Allegro is a streamlined approach specifically designed to help organizations perform risk assessments that are efficient and effective, particularly when handling information assets. The methodology focuses on a thorough examination of information assets, the threats they face, and the impact of those threats.
Activity Area 1: OCTAVE Allegro defines the criteria for evaluating the impact of risks, which is consistent with determining the risk effects' evaluation criteria in the scenario.
Activity Area 2: In OCTAVE Allegro, a critical step is creating profiles for information assets, identifying their owners, and determining security requirements. This aligns with the activity in which Biotide identifies critical assets, their owners, and their security needs.
Activity Area 3: Identifying areas of concern that initiate risk identification and analyzing threat scenarios is central to OCTAVE Allegro. This is reflected in the activity of identifying areas of concern and determining the likelihood of threats.
Activity Area 4: Evaluating the risks, reviewing criteria, and determining risk levels corresponds to the latter stages of OCTAVE Allegro, where risks are prioritized based on the likelihood and impact, and risk management strategies are formulated accordingly.
The steps outlined align with the OCTAVE Allegro approach, which focuses on understanding and addressing information security risks comprehensively and in line with organizational objectives. Hence, option A, OCTAVE Allegro, is the correct answer.
ISO/IEC 27005:2018 emphasizes the importance of using structured methodologies for information security risk management, like OCTAVE Allegro, to ensure that risks are consistently identified, assessed, and managed in accordance with organizational risk tolerance and objectives.

NEW QUESTION # 27
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. Managerial
- B. Technical
- C. Administrative

Answer: C

Explanation:
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 # 28
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
	Critical asset: Electronic health records that are tracked to analyze trends during the development of new drugs.		
Main impact areas are: • Reputation • Customer confidence • Legal fines There are three possible levels of impact for these areas: • Low • Moderate • High	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 determine the probability of threat scenarios
- B. To evaluate the potential impact of the risk on Biotide's objectives
- C. To identify the assets on which information is stored

Answer: B

Explanation:
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 # 29
Which of the following statements best defines information security risk?

- A. Potential cause of an unwanted incident related to information security that can cause harm to an organization
- B. The potential that threats will exploit vulnerabilities of an information asset and cause harm to an organization
- C. Weakness of an asset or control that can be exploited by one or a group of threats

Answer: B

Explanation:
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 # 30
.....

To help you prepare well, we offer three formats of our ISO-IEC-27005-Risk-Manager exam product. These formats include PECB ISO-IEC-27005-Risk-Manager PDF dumps, Desktop Practice Tests, and web-based PECB Certified ISO/IEC 27005 Risk Manager (ISO-IEC-27005-Risk-Manager) practice test software. Our efficient customer service is available 24/7 to support you in case of trouble while using our ISO-IEC-27005-Risk-Manager Exam Dumps. Check out the features of our formats.