Free Questions for ISO-IEC-27005-Risk-Manager

Shared by Taylor on 04-09-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

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.

Question 2

Question Type: MultipleChoice

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
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.

Which risk assessment methodology does Biotide use?

Options:

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

Answer:

A

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.

Question 3

Question Type: MultipleChoice

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.

Options:

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

Explanation:

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.

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.

Question 4

Question Type: MultipleChoice

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, Productscape decided to accept the residual risk and risk owners were assigned the responsibility of managing this risk.

Based on the guidelines of ISO/IEC 27005, is this acceptable?

Options:

A- Yes, risk owners must be aware of the residual risk and accept the responsibility for managing

it

B- No, risk approvers are responsible for managing the residual risk after accepting it

C- No, the top management should manage the residual risk

Answer:

A

Explanation:

ISO/IEC 27005 specifies that once a risk treatment has been applied and residual risk remains, it is essential that the risk owner is aware of this residual risk and accepts the responsibility for managing it. The risk owner is the individual or entity accountable for managing specific risks within the organization. In Scenario 6, Productscape decided to accept the residual risk and assigned risk owners the responsibility for managing it, which is fully compliant with ISO/IEC 27005. Thus, the correct answer is A.

ISO/IEC 27005:2018, Clause 8.6, 'Risk Treatment,' which states that risk owners should be aware of and accept responsibility for managing residual risks.

Question 5

Question Type: MultipleChoice

What should an organization do after it has established the risk communication plan?

Options:

A- Change the communication approach and tools

B- Update the information security policy

C- Establish internal and external communication

Answer:

C

Explanation:

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.

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.

Question 6

Question Type: MultipleChoice

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, which principle of efficient communication strategy Adstry's project managers follow when communicating risks to team members?

Options:

A- Clarity
B- Credibility
C- Responsiveness

Answer:

A

Explanation:

Adstry's project managers focus on ensuring that the information provided to team members is communicated using an appropriate language that can be understood by all. This approach reflects the principle of clarity, which is a key element of an effective communication strategy. Clear communication helps to ensure that all parties understand the risks, their implications, and the necessary actions to mitigate them. Option B (Credibility) relates to trustworthiness, which is not the primary focus here, and Option C (Responsiveness) involves timely reactions, which is also not the main point of emphasis in this context.

Question 7

Question Type: MultipleChoice

According to CRAMM methodology, how is risk assessment initiated?

Options:

A- By gathering information on the system and identifying assets within the scope
B- By identifying the security risks
C- By determining methods and procedures for managing risks

Answer:

A

Explanation:

According to the CRAMM (CCTA Risk Analysis and Management Method) methodology, risk assessment begins by collecting detailed information on the system and identifying all assets that fall within the defined scope. This foundational step ensures that the assessment is comprehensive and includes all relevant assets, which could be potential targets for risk. This makes option A the correct answer.

Question 8

Question Type: MultipleChoice

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 the scenario above, answer the following question:

Which risk treatment option was used for the first risk scenario?

Options:

A- Risk modification
B- Risk avoidance
C- Risk sharing

Answer:

A

Explanation:

Risk modification involves implementing measures to reduce the likelihood or impact of a risk. In the first risk scenario, Productscape decided to use an automated 'build and deploy' process to reduce the likelihood of an attacker exploiting a security misconfiguration vulnerability. This action aims to lower the risk to an acceptable level, which is characteristic of risk modification. Option B (Risk avoidance) would involve eliminating the risk by avoiding the activity altogether, which is not what was done. Option C (Risk sharing) involves transferring some or all of the risk to a third party, which is not applicable in this scenario.

Question 9

Question Type: MultipleChoice

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 the table provided in scenario 8, did Biotide follow all the steps of the risk assessment methodology regarding the identification of assets?

Options:

A- No, Biotide should identify only critical assets and electronic health records is not a critical asset

B- No, after identifying critical assets, Biotide should define the asset owners

C- Yes, the identification of assets involves only the identification of critical information assets and their security requirements

Answer:

B

Explanation:

Based on the scenario, Biotide follows a methodology where the identification of critical assets is part of Activity Area 2. However, according to ISO/IEC 27005, after identifying the critical assets, the organization should also identify and document the asset owners.

ISO/IEC 27005:2018 emphasizes that the asset owner is responsible for the protection of the asset and that understanding ownership is critical to implementing effective risk management controls. In the given table, the scenario does not explicitly mention defining the asset owners after identifying critical assets, which is a necessary step. Therefore, the correct answer is B.

ISO/IEC 27005:2018, Section 7.2.2 'Identification of assets, owners, and risk sources' details the steps required for proper asset identification, including defining the asset owners as a critical part of the risk assessment process.

Question 10

Question Type: MultipleChoice

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?

Options:

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

Explanation:

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.

Question 11

Question Type: MultipleChoice

According to ISO/IEC 27005, what is the output of the documentation of risk management processes?

Options:

A- Knowledge on the information security risk assessment and treatment processes in accordance with clauses 7 and 8 of the standard
B- Documented information about the information security risk assessment and treatment results
C- Documented information that is necessary for the effectiveness of the information security risk assessment or risk treatment processes

Answer:

B

Explanation:

According to ISO/IEC 27005, the output of the documentation of risk management processes should include detailed information about the results of the risk assessment and the chosen risk treatment options. This ensures transparency and provides a clear record of the decision-making process related to information security risk management. Therefore, option B is the correct answer.

Question 12

Question Type: MultipleChoice

Based on the EBIOS RM method, which of the following is one of the four attack sequence phases?

Options:

A- Exploiting
B- Treating
C- Attacking

Answer:

A

Explanation:

Based on the EBIOS Risk Manager (EBIOS RM) methodology, the attack sequence phases include

various steps that an attacker might take to compromise an organization's assets. The four phases generally cover reconnaissance, exploiting vulnerabilities, achieving objectives, and maintaining persistence. 'Exploiting' is specifically the phase where the attacker takes advantage of identified vulnerabilities in the system, which directly aligns with option A.