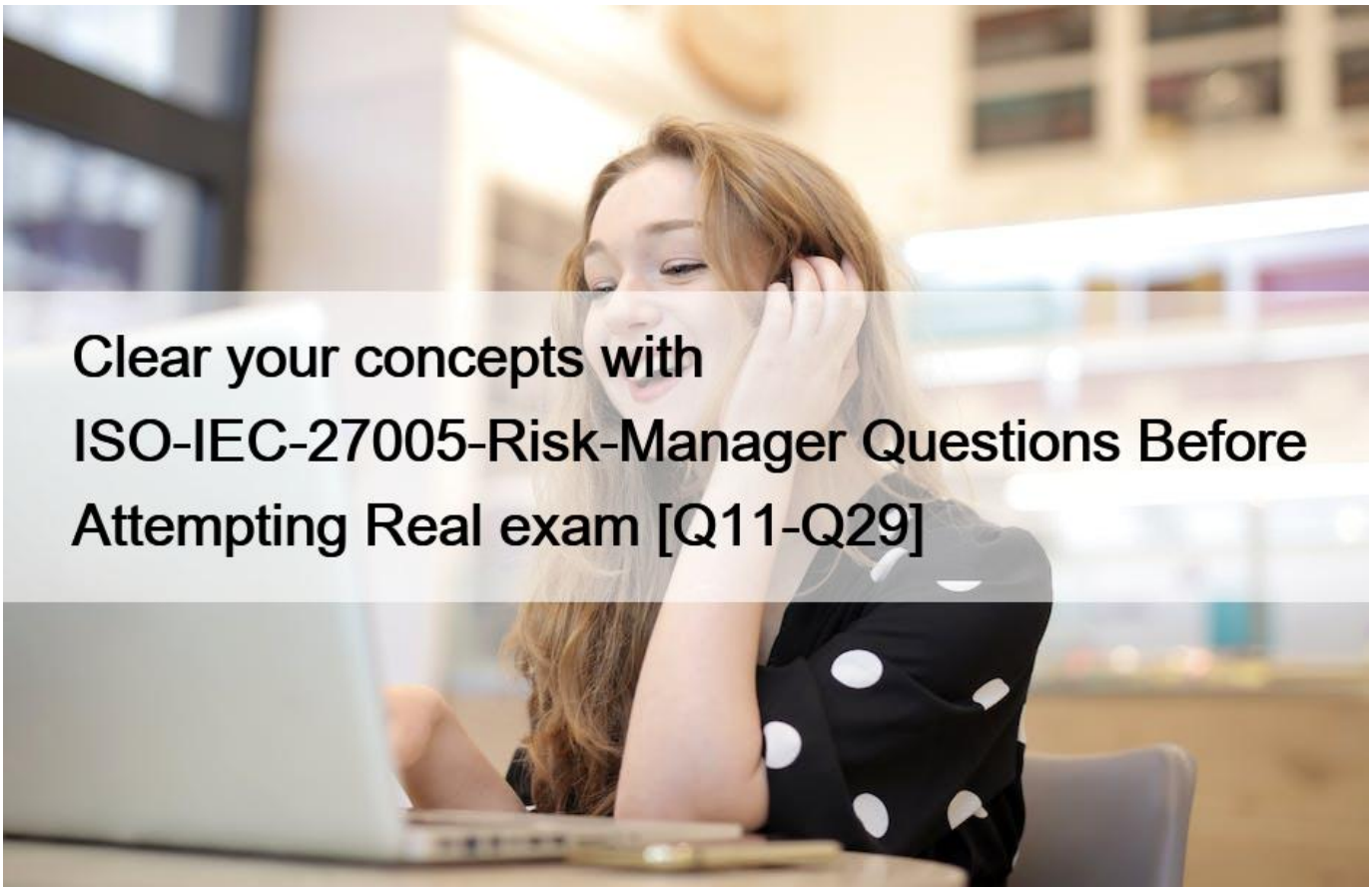
Clear your concepts with ISO-IEC-27005-Risk-Manager Questions Before Attempting Real exam [Q11-Q29



Clear your concepts with ISO-IEC-27005-Risk-Manager Questions Before Attempting Real exam
Get professional help from our ISO-IEC-27005-Risk-Manager Dumps PDF

Q11. 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?
* Clarity
* Credibility
* Responsiveness

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.

Q12. 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?
* Technical
* Managerial
* Administrative

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.

Q13. Scenario 2: Travivve is a travel agency that operates in more than 100 countries. Headquartered in San Francisco, the US, the agency is known for its personalized vacation packages and travel services. Travivve aims to deliver reliable services that meet its clients’ needs. Considering the impact of information security in its reputation, Travivve decided to implement an information security management system (ISMS) based on ISO/IEC 27001. In addition, they decided to establish and implement an information security risk management program. Based on the priority of specific departments in Travivve, the top management decided to initially apply the risk management process only in the Sales Management Department. The process would be applicable for other departments only when introducing new technology.

Travivve’s top management wanted to make sure that the risk management program is established based on the industry best practices. Therefore, they created a team of three members that would be responsible for establishing and implementing it. One of the team members was Travivve’s risk manager who was responsible for supervising the team and planning all risk management activities. In addition, the risk manager was responsible for monitoring the program and reporting the monitoring results to the top management.

Initially, the team decided to analyze the internal and external context of Travivve. As part of the process of understanding the organization and its context, the team identified key processes and activities. Then, the team identified the interested parties and their basic requirements and determined the status of compliance with these requirements. In addition, the team identified all the reference documents that applied to the defined scope of the risk management process, which mainly included the Annex A of ISO/IEC 27001 and the internal security rules established by Travivve. Lastly, the team analyzed both reference documents and justified a few noncompliances with those requirements.

The risk manager selected the information security risk management method which was aligned with other approaches used by the company to manage other risks. The team also communicated the risk management process to all interested parties through previously established communication mechanisms. In addition, they made sure to inform all interested parties about their roles and responsibilities regarding risk management. Travivve also decided to involve interested parties in its risk management activities since, according to the top management, this process required their active participation.

Lastly, Travivve’s risk management team decided to conduct the initial information security risk assessment process. As such, the team established the criteria for performing the information security risk assessment which included the consequence criteria and likelihood criteria.

Based on scenario 2, has Travivve defined the responsibilities of the risk manager appropriately?
* Yes, the risk manager should be responsible for all actions defined bv Traviwe
* No, the risk manager should not be responsible for planning all risk management activities
* No, the risk manager should not be responsible for reporting the monitoring results of the risk management program to the top management

ISO/IEC 27005 recommends that the risk manager or a designated authority should oversee the entire risk management process, including planning, monitoring, and reporting. In the scenario, the risk manager is responsible for supervising the team, planning all risk management activities, monitoring the program, and reporting the results to top management. This allocation of responsibilities is aligned with the guidelines of ISO/IEC 27005, which emphasizes that a risk manager should coordinate and manage all aspects of the risk management process to ensure its effectiveness and alignment with the organization’s objectives. Therefore,

assigning these responsibilities to the risk manager is appropriate, making option A the correct answer.

Reference:

ISO/IEC 27005:2018, Clause 5.3, “Roles and responsibilities,” which specifies that those managing risk should have defined roles and should coordinate all activities in the risk management process.

Q14. 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.

Which of the following situations indicates that Printary identified consequences of risk scenarios? Refer to scenario 3.
* Printary concluded that the complicated user interface could increase the risk of user error and impact data integrity and confidentiality
* Printary used the list of potential incident scenarios and assessed their impact on company’s information security
* Printary identified two main threats associated with the online payment system: error in use and corruption of data
According to ISO/IEC 27005, the risk management process involves identifying, analyzing, and evaluating risks in a structured manner. Specifically, risk identification entails recognizing potential threats, vulnerabilities, and consequences to information assets. Once risks are identified, ISO/IEC 27005 emphasizes the importance of risk analysis, where risks are assessed in terms of their potential consequences and likelihood.

In the scenario, Printary followed this structured approach, aligning with the ISO/IEC 27005 framework. First, they identified the threats associated with the online payment system, which were categorized as user errors and data corruption. However, identification of threats alone does not equate to identifying the consequences of risk scenarios, as required by the risk analysis phase in ISO/IEC 27005.

The key to recognizing that Printary identified the consequences lies in the fact that they “used the list of potential incident

scenarios and assessed their impact on the company’s information security.” This directly corresponds to ISO/IEC 27005’s guidelines on risk analysis, where organizations must evaluate both the likelihood and the impact (consequences) of potential incidents on their assets. In other words, by assessing the impact of the incident scenarios, Printary is analyzing the consequences of the identified risks, which is a crucial step in the risk analysis process.

Option A refers to identifying a risk (user error leading to compromised data integrity and confidentiality), but this does not constitute a comprehensive analysis of the risk’s consequences as per ISO/IEC 27005. Similarly, Option C highlights the identification of threats, but the threats themselves are not the consequences of risk scenarios.

Thus, Option B is the most accurate as it reflects Printary’s alignment with ISO/IEC 27005 guidelines in assessing the potential consequences of risk scenarios by evaluating their impact on the company’s information security.

Q15. 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, Adstry’s project managers hold regular meetings with interested parties to discuss risks and risk treatment solutions. According to the guidelines of ISO/IEC 27005, is this in compliance with best practices?
* No, risk owners should not communicate or discuss risk treatment options with external interested parties
* Yes, the coordination between project managers and relevant interested parties can be achieved by discussions upon risks and appropriate treatment solutions
* Yes, risks can be communicated to and discussed with relevant interested parties only if the project manager decides that it is appropriate to do so

Q16. According to ISO/IEC 27000, what is the definition of information security?
* Preservation of confidentiality, integrity, and availability of information
* Protection of privacy during the processing of personally identifiable information
* Preservation of authenticity, accountability, and reliability in the cyberspace
According to ISO/IEC 27000, information security is defined as the “preservation of confidentiality, integrity, and availability of information.” This definition highlights the three core principles of information security:

Confidentiality ensures that information is not disclosed to unauthorized individuals or systems.

Integrity ensures the accuracy and completeness of information and its processing methods.

Availability ensures that authorized users have access to information and associated assets when required.

This definition encompasses the protection of information in all forms and aligns with ISO/IEC 27005’s guidelines on managing information security risks. Therefore, option A is the correct answer. Options B and C are incorrect as they refer to more specific aspects or other areas of information management.

Q17. Based on NIST Risk Management Framework, what is the last step of a risk management process?
* Monitoring security controls
* Accessing security controls
* Communicating findings and recommendations
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.

Q18. 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.

How should Detika define which of the identified risks should be treated first? Refer to scenario 5.
* Based on their priority in the risk treatment plan
* Based on the resources required for ensuring effective implementation
* Based on who is accountable and responsible for approving the risk treatment plan
Detika should prioritize the treatment of identified risks based on their priority in the risk treatment plan. According to ISO/IEC 27005, the risk treatment plan specifies the order in which risks should be treated based on their severity, likelihood, and impact on the organization. Risks that pose the greatest threat to the organization or have the highest priority should be treated first. Options B and C are incorrect because allocating resources or determining accountability do not inherently establish the priority of risk treatment; the risk treatment plan does.

Q19. Scenario 2: Travivve is a travel agency that operates in more than 100 countries. Headquartered in San Francisco, the US, the agency is known for its personalized vacation packages and travel services. Travivve aims to deliver reliable services that meet its clients’ needs. Considering the impact of information security in its reputation, Travivve decided to implement an information security management system (ISMS) based on ISO/IEC 27001. In addition, they decided to establish and implement an information security risk management program. Based on the priority of specific departments in Travivve, the top management decided to initially apply the risk management process only in the Sales Management Department. The process would be applicable for other departments only when introducing new technology.

Travivve’s top management wanted to make sure that the risk management program is established based on the industry best practices. Therefore, they created a team of three members that would be responsible for establishing and implementing it. One of the team members was Travivve’s risk manager who was responsible for supervising the team and planning all risk management activities. In addition, the risk manager was responsible for monitoring the program and reporting the monitoring results to the top management.

Initially, the team decided to analyze the internal and external context of Travivve. As part of the process of understanding the organization and its context, the team identified key processes and activities. Then, the team identified the interested parties and their basic requirements and determined the status of compliance with these requirements. In addition, the team identified all the reference documents that applied to the defined scope of the risk management process, which mainly included the Annex A of ISO/IEC 27001 and the internal security rules established by Travivve. Lastly, the team analyzed both reference documents and justified a few noncompliances with those requirements.

The risk manager selected the information security risk management method which was aligned with other approaches used by the company to manage other risks. The team also communicated the risk management process to all interested parties through previously established communication mechanisms. In addition, they made sure to inform all interested parties about their roles and responsibilities regarding risk management. Travivve also decided to involve interested parties in its risk management activities since, according to the top management, this process required their active participation.

Lastly, Travivve’s risk management team decided to conduct the initial information security risk assessment process. As such, the team established the criteria for performing the information security risk assessment which included the consequence criteria and likelihood criteria.

Did the risk management team establish all the criteria required to perform the information security risk assessment? Refer to scenario 2.
* No, the risk management team should also establish the criteria for determining the level of risk
* No, the risk management team should also establish the criteria for treating the identified risks
* Yes. the risk management team established all the criteria that are necessary to perform an information security risk assessment
While Travivve’s risk management team established criteria for consequence and likelihood, ISO/IEC 27005 requires that additional criteria should be defined to complete a risk assessment. Specifically, the team should also establish criteria for determining the level of risk, which involves combining the likelihood and consequence to evaluate risk magnitude. This step is crucial for prioritizing risks and determining which risks require treatment. The absence of criteria for determining the level of risk

means that the team did not fully meet the requirements of ISO/IEC 27005 for performing an information security risk assessment. Therefore, the correct answer is A.

Reference:

ISO/IEC 27005:2018, Clause 8.4, “Risk Assessment,” which outlines the need to establish criteria for risk acceptance, which includes determining the level of risk.

Q20. Does information security reduce the impact of risks?
* Yes, information security reduces risks and their impact by protecting the organization against threats and vulnerabilities
* No, information security does not have an impact on risks as information security and risk management are separate processes
* Yes, information security reduces the impact of risks by eliminating the likelihood of exploitation of vulnerabilities by threats

Information security aims to protect information assets against threats and vulnerabilities that could lead to unauthorized access, disclosure, alteration, or destruction. By implementing effective security measures (such as access controls, encryption, and monitoring), an organization reduces the likelihood of vulnerabilities being exploited and mitigates the potential impact of risks. According to ISO/IEC 27005, risk management in information security includes identifying, assessing, and applying controls to reduce both the likelihood and impact of potential risks. Thus, option A is correct because it acknowledges the role of information security in reducing the impact of risks. Option B is incorrect because information security is a key component of risk management, and option C is incorrect because information security does not eliminate risks entirely; it mitigates their impact.

Q21. According to CRAMM methodology, how is risk assessment initiated?
* By gathering information on the system and identifying assets within the scope
* By identifying the security risks
* By determining methods and procedures for managing risks

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.

Q22. 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, which type of assets was identified during the risk identification process?
* Tangible assets
* Primary assets
* Supporting assets

During the risk identification process, Poshoe identified the information that was vital to the achievement of the organization’s mission and objectives. Such information is considered a primary asset because it directly supports the organization’s core business objectives. Primary assets are those that are essential to the organization’s functioning and achieving its strategic goals. Option A (Tangible assets) refers to physical assets like hardware or facilities, which is not relevant here. Option C (Supporting assets) refers to assets that support primary assets, like IT infrastructure or software, which also does not fit the context.

Q23. 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, which risk treatment option did Detika select to treat the risk of a potential ransomware attack?
* Risk retention
* Risk avoidance
* Risk sharing

Risk retention involves accepting the risk when its likelihood or impact is low, or when the cost of mitigating the risk is higher than the benefit. In the scenario, Detika decided to accept the risk of a potential ransomware attack because the data is backed up daily, and additional measures were deemed unnecessary. This decision aligns with the risk retention strategy, where an organization chooses to live with the risk rather than apply further controls. Option A is the correct answer.

Reference:

ISO/IEC 27005:2018, Clause 8.6, “Risk Treatment,” which discusses risk retention as an option for managing risks deemed acceptable by the organization.

Q24. 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, the top management of Poshoe decided to treat the risk immediately after conducting the risk analysis. Is this in compliance with risk management best practices?
* No, risk evaluation should be performed before making any decision regarding risk treatment
* Yes. risk treatment options should be implemented immediately after analyzing the risk, as the risk could expose the company to other security threats
* No, the risk should be communicated to all the interested parties before making any decision regarding risk treatment
According to ISO/IEC 27005, after conducting risk analysis, the next step in the risk management process should be risk evaluation. Risk evaluation involves comparing the estimated level of risk against risk criteria established by the organization to determine the significance of the risk and decide whether it is acceptable or needs treatment. Only after evaluating the risk should an organization decide on the appropriate risk treatment options. Therefore, in the scenario, deciding to treat the risk immediately after conducting the risk analysis, without first performing a risk evaluation, is not in compliance with risk management best practices. Option A is the correct answer.

Reference:

ISO/IEC 27005:2018, Clause 8.5, “Risk Evaluation,” which describes the process of evaluating risks after analysis to determine if they require treatment.

Q25. 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, Adstry’s project managers hold regular meetings with interested parties to discuss risks and risk treatment solutions. According to the guidelines of ISO/IEC 27005, is this in compliance with best practices?
* Yes, the coordination between project managers and relevant interested parties can be achieved by discussions upon risks and appropriate treatment solutions
* Yes, risks can be communicated to and discussed with relevant interested parties only if the project manager decides that it is appropriate to do so
* No, risk owners should not communicate or discuss risk treatment options with external interested parties
According to ISO/IEC 27005, effective risk management includes communication and consultation with relevant interested parties. Holding regular meetings to discuss risks, their prioritization, and appropriate treatment solutions is a good practice for ensuring that all parties are aware of the risks and involved in the decision-making process for risk treatment. This approach fosters coordination and collaboration, which is essential for managing risks effectively. Therefore, the practice of discussing risks and treatment options with relevant interested parties aligns with best practices, making option A the correct answer.

Reference:

ISO/IEC 27005:2018, Clause 7, “Communication and Consultation,” which emphasizes the importance of communicating risks and consulting with relevant interested parties.

Q26. 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, project managers communicate risks to external interested parties, taking into account the information confidentiality. Which principle of efficient communication strategy do project managers follow?
* Credibility
* Responsiveness
* Transparency

ISO/IEC 27005 emphasizes that effective risk management involves clear communication strategies, especially when it comes to ensuring that all stakeholders-both internal and external-are well-informed about potential risks and their impacts. The communication of risks is an essential part of the risk treatment process, as stated in the ISO/IEC 27005 standard.

In the given scenario, Adstry project managers are responsible for communicating risks to external interested parties, while carefully considering the confidentiality of the company’s information. They ensure that the risks are conveyed with the appropriate level of detail, protecting sensitive information but still providing the necessary insights to interested parties. This level of disclosure ensures that stakeholders are well aware of the risks without compromising the organization’s confidentiality policies.

The principle of transparency in communication refers to the clear, open, and honest sharing of information that stakeholders need in order to make informed decisions. By identifying interested parties, considering their concerns, and ensuring risk communication is well-prepared and detailed appropriately, Adstry’s project managers are practicing transparency. They provide the necessary risk information while balancing the protection of confidential data.

Option A, credibility, refers to building trust in communication, which is not the primary focus in this context. Option B, responsiveness, is about timely reactions to risks or concerns but doesn’t directly relate to how the information is communicated regarding risk confidentiality.

Thus, transparency is the correct answer because it aligns with how project managers ensure that the necessary risk details are

communicated in a clear and honest way, while still protecting confidential information, as outlined by ISO/IEC 27005 risk communication principles.

Q27. 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 scenario 3, Printary used a list of identified events that could negatively influence the achievement of its information security objectives to identify information security risks. Is this in compliance with the guidelines of ISO/IEC 27005?
* No, a list of risk scenarios with their consequences related to assets or events and their likelihood should be used to identity information security risks
* Yes, a list of events that can negatively influence the achievement of information security objectives in the company should be used to identity information security risks
* No. a list of risk sources, business processes. and business objectives should be used to identify information security risks
According to ISO/IEC 27005, identifying risks to information security involves recognizing events that could adversely affect the achievement of information security objectives. Using a list of events that could negatively impact these objectives is consistent with the risk identification process as outlined in ISO/IEC 27005. This approach focuses on identifying specific incidents or events that could result in security breaches or compromises, providing a clear understanding of the potential risks to the organization. Thus, Printary’s use of a list of such events to identify information security risks complies with the standard’s guidelines, making option B the correct answer.

Reference:

ISO/IEC 27005:2018, Clause 8.2, “Risk Identification,” which states that the organization should identify the events that could compromise information security objectives.

Q28. 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.

Based on the scenario above, answer the following question:

Bontton established a risk management process based on ISO/IEC 27005, to systematically manage information security threats. Is this a good practice?
* Yes, ISO/IEC 27005 provides guidelines for information security risk management that enable organizations to systematically manage information security threats
* Yes, ISO/IEC 27005 provides guidelines to systematically manage all types of threats that organizations may face
* No, ISO/IEC 27005 cannot be used to manage information security threats in the food sector
ISO/IEC 27005 is the standard that provides guidelines for information security risk management, which supports the requirements of an Information Security Management System (ISMS) as specified in ISO/IEC 27001. In the scenario provided, Bontton established a risk management process to identify, analyze, evaluate, and treat information security risks, which is in alignment with the guidelines set out in ISO/IEC 27005. The standard emphasizes a systematic approach to identifying assets, identifying threats and vulnerabilities, assessing risks, and implementing appropriate risk treatment measures, such as training and awareness sessions. Thus, option A is correct, as it accurately reflects the purpose and application of ISO/IEC 27005 in managing information security threats. Option B is incorrect because ISO/IEC 27005 specifically addresses information security threats, not all types of threats, and option C is incorrect because ISO/IEC 27005 is applicable to any sector, including the food industry, as long as it concerns information security risks.

Q29. Scenario 2: Travivve is a travel agency that operates in more than 100 countries. Headquartered in San Francisco, the US, the agency is known for its personalized vacation packages and travel services. Travivve aims to deliver reliable services that meet its clients’ needs. Considering the impact of information security in its reputation, Travivve decided to implement an information security management system (ISMS) based on ISO/IEC 27001. In addition, they decided to establish and implement an information security risk management program. Based on the priority of specific departments in Travivve, the top management decided to initially apply the risk management process only in the Sales Management Department. The process would be applicable for other departments only when introducing new technology.

Travivve’s top management wanted to make sure that the risk management program is established based on the industry best practices. Therefore, they created a team of three members that would be responsible for establishing and implementing it. One of the team members was Travivve’s risk manager who was responsible for supervising the team and planning all risk management activities. In addition, the risk manager was responsible for monitoring the program and reporting the monitoring results to the top management.

Initially, the team decided to analyze the internal and external context of Travivve. As part of the process of understanding the organization and its context, the team identified key processes and activities. Then, the team identified the interested parties and their basic requirements and determined the status of compliance with these requirements. In addition, the team identified all the reference documents that applied to the defined scope of the risk management process, which mainly included the Annex A of ISO/IEC 27001 and the internal security rules established by Travivve. Lastly, the team analyzed both reference documents and justified a few noncompliances with those requirements.

The risk manager selected the information security risk management method which was aligned with other approaches used by the company to manage other risks. The team also communicated the risk management process to all interested parties through previously established communication mechanisms. In addition, they made sure to inform all interested parties about their roles and responsibilities regarding risk management. Travivve also decided to involve interested parties in its risk management activities since, according to the top management, this process required their active participation.

Lastly, Travivve’s risk management team decided to conduct the initial information security risk assessment process. As such, the team established the criteria for performing the information security risk assessment which included the consequence criteria and likelihood criteria.

Based on scenario 2, the team decided to involve interested parties in risk management activities. Is this a good practice?
* No. only internal interested parties should be involved in risk management activities
* Yes, relevant interested parties should be involved in risk management activities to ensure the successful completion of the risk assessment
* No, only the risk management team should be involved in risk management activities
According to ISO/IEC 27005, involving relevant interested parties in the risk management process is considered a best practice. This approach ensures that all perspectives are considered, and relevant knowledge is leveraged, which helps in comprehensively identifying, analyzing, and managing risks. Interested parties, such as stakeholders, can provide valuable insights and information regarding the organization’s assets, processes, threats, and vulnerabilities, contributing to a more accurate and effective risk assessment. Therefore, option B is correct because it supports the principle that involving relevant parties leads to a more successful risk assessment process. Options A and C are incorrect because excluding either external interested parties or restricting involvement only to the risk management team would limit the effectiveness of the risk management process.