ISACA.CRISC.v2022-10-10.q527

Exam Code:	CRISC
Exam Name:	Certified in Risk and Information Systems Control
Certification Provider:	ISACA
Free Question Number:	527
Version:	v2022-10-10
# of views:	8120
# of Questions views:	5270
https://www.exam-tests.com/CRISC-exam/ISACA.CRISC.v2022-10-10.q527.html	

NEW QUESTION: 1
Mitigating technology risk to acceptable levels should be based PRIMARILY upon:
A. business sector best practices.
B. availability of automated solutions.
C. organizational risk appetite.
D. business process requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following would BEST indicate to senior management that IT processes are improving?
A. Changes in the number of security exceptions
B. Changes to the structure of the risk register
C. Changes in the number of intrusions detected
D. Changes in the position in the maturity model
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following operational risks ensures that the provision of a quality product is not overshadowed by the production costs of that product?
A. Information security risks
B. Contract and product liability risks
C. Project activity risks
D. Profitability operational risks
Answer: D (LEAVE A REPLY)
Section: Volume B
Explanation/Reference:

Explanation:
Profitability operational risks focus on the financial risks which encompass providing a quality product that is cost-effective in production. It ensures that the provision of a quality product is not overshadowed by the production costs of that product.
Incorrect Answers:
A: Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security risks are the risks that are associated with the protection of these information and information systems.
B: These risks do not ensure that the provision of a quality product is not overshadowed by the production costs of that product.
C: Project activity risks are not associated with provision of a quality product or the production costs of that product.

NEW QUESTION: 4
Which of the following test is BEST to map for confirming the effectiveness of the system access management process?
A. user accounts to human resources (HR) records.
B. user accounts to access requests.
C. the vendor database to user accounts.
D. access requests to user accounts.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Tying user accounts to access requests confirms that all existing accounts have been approved. Hence, the effectiveness of the system access management process can be accounted.
Incorrect Answers:
A: Tying user accounts to human resources (HR) records confirms whether user accounts are uniquely tied to employees, not accounts for the effectiveness of the system access management process.
C: Tying vendor records to user accounts may confirm valid accounts on an e-commerce application, but it does not consider user accounts that have been established without the supporting access request.
D: Tying access requests to user accounts confirms that all access requests have been processed; however, the test does not consider user accounts that have been established without the supporting access request.

NEW QUESTION: 5
Which of the following approaches BEST identifies information systems control deficiencies?
A. Countermeasures analysis
B. Gap analysis

C. Risk assessment
D. Best practice assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 6
What activity should be done for effective post-implementation reviews during the project?
A. Establish the business measurements up front
B. Allow a sufficient number of business cycles to be executed in the new system
C. Identify the information collected during each stage of the project
D. Identify the information to be reviewed
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
For effective post-implementation review the business measurements up front is established during the project.
Incorrect Answers:
B: Executing sufficient number of business cycles in the new system is done after the completion of the project.
C, D: Identifying the information to be reviewed and information collected during each stage of project is done in pre-project phase and not during project for effective post-implementation review.

NEW QUESTION: 7
What are the responsibilities of the CRO?
Each correct answer represents a complete solution. Choose three.
A. Managing the supporting risk management function
B. Managing the risk assessment process
C. Advising Board of Directors
D. Implement corrective actions
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Chief Risk Officer is the executive-level manager in an organization. They provide corporate, guidance, governance, and oversight over the enterprise's risk management activities. The main priority for the CRO is to ensure that the organization is in full compliance with applicable regulations. They may also deal with areas regarding insurance, internal auditing, corporate investigations, fraud, and information security.
CRO's responsibilities include:
Managing the risk assessment process
Implementation of corrective actions

Communicate risk management issues
- Supporting the risk management functions
-

NEW QUESTION: 8
You are the project manager of the GHY project for your company. This project has a budget of $543,000 and is expected to last 18 months. In this project, you have identified several risk events and created risk response plans. In what project management process group will you implement risk response plans?
A. Monitoring and Controlling
B. In any process group where the risk event resides
C. Planning
D. Executing
E. Explanation:
The monitor and control project risk process resides in the monitoring and controlling project management process group. This process is responsible for implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness through the project.
F. is incorrect. Risk response plans are not implemented as part of project planning.
G. is incorrect. Risk response plans are not implemented as part of project execution.
Answer: (SHOW ANSWER)
is incorrect. Risk response plans are implemented as part of the monitoring and controlling process group.

NEW QUESTION: 9
The PRIMARY reason for tracking the status of risk mitigation plans is to ensure:
A. compliance with corporate policies.
B. the risk response strategy has been decided.
C. the proposed controls are implemented as scheduled.
D. security controls are tested prior to implementation.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
Which of the following BEST indicates effective information security incident management?
A. Frequency of information security incident response plan testing
B. Percentage of high risk security incidents
C. Average time to identify critical information security incidents
D. Monthly trend of information security-related incidents
Answer: (SHOW ANSWER)

NEW QUESTION: 11

Which of the following would BEST help an enterprise define and communicate its risk appetite?
A. Risk assessment
B. Gap analysis
C. Heat map
D. Risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 12
A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:
A. modify internal assurance activities to include control validation.
B. conduct a gap analysis against compliance criteria.
C. identify necessary controls to ensure compliance.
D. collaborate with management to meet compliance requirements.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 13
While evaluating control costs, management discovers that the annual cost exceeds the annual loss expectancy (ALE) of the risk. This indicates the:
A. control is ineffective and should be strengthened
B. risk is inefficiently controlled
C. risk is efficiently controlled
D. control is weak and should be removed
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 14
You are the project manager for Bluewell Inc. You are studying the documentation of project plan. The documentation states that there are twenty-five stakeholders with the project. What will be the number of communication channel s for the project?
A. 20
B. 100
C. 50
D. 300
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Communication channels are paths of communication with stakeholders in a project. The number of communication channels shows the complexity of a project's communication and can be derived through the formula shown below:
Total Number of Communication Channels = n (n-1)/2

where n is the number of stakeholders.
Hence, a project having five stakeholders will have ten communication channels. Putting the value of the number of stakeholders in the formula will provide the number of communication channels.
Hence,
Number of communication channel = (n (n-1)) / 2
= (25 (25-1)) / 2
= (25 x 24) / 2
= 600 / 2
= 300
Incorrect Answers:
A, B, C: These are not valid number of communication channels for the given scenario.

NEW QUESTION: 15
Ned is the project manager of the HNN project for your company. Ned has asked you to help him complete some probability distributions for his project. What portion of the project will you most likely use for probability distributions?
A. Bias towards risk in new resources
B. Risk probability and impact matrixes
C. Uncertainty in values such as duration of schedule activities
D. Risk identification
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risk probability distributions are likely to be utilized in uncertain values, such as time and cost estimates for a project.
Incorrect Answers:
A: Risk probability distributions do not typically interact with the bias towards risks in new resources.
B: Risk probability distributions are not likely to be used with risk probability and impact matrices.
D: Risk probability distributions are not likely the risk identification.

NEW QUESTION: 16
Which among the following is the MOST crucial part of risk management process?
A. Risk communication
B. Auditing
C. Risk monitoring
D. Risk mitigation
E. Explanation:
Risk communication is a critical part in the risk management process. People are naturally uncomfortable talking about risk and tend to put off admitting that risk is involved and

communicating about issues; incidents; and; eventually, even crises.
If risk is to be managed and mitigated, it must first be discussed and effectively communicated throughout an enterprise.
F. is incorrect. Risk mitigation is one of the phases of risk management process for effective mitigation of risk it should be first communicated throughout an enterprise.
G. is incorrect. Auditing is done to test the overall risk management process and the planned risk responses. So it is the very last phase after completion of risk management process.
Answer: A (LEAVE A REPLY)
is incorrect. Risk monitoring is the last phase to complete risk management process, and for proper management of risk it should be communicated properly. Hence risk communication is the most crucial step.

NEW QUESTION: 17
The analysis of which of the following will BEST help validate whether suspicious network activity is malicious?
A. Intrusion detection system (IDS) rules
B. Penetration test reports
C. Vulnerability assessment reports
D. Logs and system events
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 18
Which of the following tools is MOST helpful when mapping IT risk management outcomes to organizational objectives?
A. Risk dashboard
B. RACI chart
C. Information security risk map
D. Strategic business plan
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 19
During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?
A. Warning signs
B. Symptoms
C. Risk rating
D. Cost of the project
Answer: D (LEAVE A REPLY)
Section: Volume B
Explanation:
The cost of the project is not an indicator of risk urgency. The affect of the risk on the overall cost of the project may be considered, but it is not the best answer.
Incorrect Answers:
A: Warning signs are an indicator of the risk urgency.
B: Symptoms are an indicator of the risk urgency.
C: The risk rating can be an indicator of the risk urgency.

NEW QUESTION: 20
When developing IT risk scenarios, it is CRITICAL to involve:
A. process owners
B. IT managers
C. internal auditors
D. senior management
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 21
Which of the following aspects are included in the Internal Environment Framework of COSO ERM?
Each correct answer represents a complete solution. Choose three.
A. Enterprise's integrity and ethical values
B. Enterprise's working environment
C. Enterprise's human resource standards
D. Enterprise's risk appetite
Answer: A,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The internal environment for risk management is the foundational level of the COSO ERM framework, which describes the philosophical basics of managing risks within the implementing enterprise. The different aspects of the internal environment include the enterprise's:
Philosophy on risk management

- Risk appetite
- Attitudes of Board of Directors
- Integrity and ethical values
- Commitment to competence
- Organizational structure
- Authority and responsibility
- Human resource standards

NEW QUESTION: 22
You and your project team are identifying the risks that may exist within your project. Some of the risks are small risks that won't affect your project much if they happen. What should you do with these identified risk events?
A. These risks can be dismissed.
B. These risks can be accepted.
C. These risks can be added to a low priority risk watch list.
D. All risks must have a valid, documented risk response.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Low-impact, low-probability risks can be added to the low priority risk watch list.
Incorrect Answers:
A: These risks are not dismissed; they are still documented on the low priority risk watch list.
B: While these risks may be accepted, they should be documented on the low priority risk watch list. This list will be periodically reviewed and the status of the risks may change.
D: Not every risk demands a risk response, so this choice is incorrect.

NEW QUESTION: 23
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:
A. treatment
B. identification
C. communication
D. assessment
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 24
What can be determined from the risk scenario chart?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Sierra	Medium	Low	Low
Tango	Medium	Low	Medium
Uniform	High	High	High
Victor	High	Medium	Medium

A. Risk treatment options
B. Relative positions on the risk map
C. Capability of enterprise to implement
D. The multiple risk factors addressed by a chosen response
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following data would be used when performing a business impact analysis (BIA)?
A. Cost of regulatory compliance
B. Projected impact of current business on future business
C. Expected costs for recovering the business
D. Cost-benefit analysis of running the current business
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
If preventive controls cannot be implemented due to technology limitations, which of the following should be done FIRST to reduce risk?
A. Redefine the business process to reduce the risk
B. Evaluate alternative controls
C. Develop a plan to upgrade technology
D. Define a process for monitoring risk
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 27
An organization's HR department has implemented a policy requiring staff members to take a minimum of five consecutive days leave per year to mitigate the risk of malicious insider activities. Which of the following is the BEST key performance indicator (KPI) of the effectiveness of this policy?
A. Percentage of staff members seeking exception to the policy
B. Financial loss incurred due to malicious activities during staff members' leave
C. Number of malicious activities occurring during staff members leave
D. Percentage of staff members taking leave according to the policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following is NOT true for effective risk communication?
A. Risk information must be known and understood by all stakeholders.
B. Use of technical terms of risk
C. Any communication on risk must be relevant
D. For each risk, critical moments exist between its origination and its potential business consequence
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation:
For effective communication, information communicated should not inundate the recipients. All ground rules of good communication apply to communication on risk. This includes the avoidance of jargon and technical terms regarding risk because the intended audiences are generally not deeply technologically skilled. Hence use of technical terms is avoided for effective communication Incorrect Answers:
A, C, D: These all are true for effective risk communication. For effective risk communication the risk information should be clear, concise, useful and timely. Risk information must be known and understood by all the stakeholders. Information or communication should not overwhelm the recipients. This includes the avoidance of technical terms regarding risk because the intended audiences are generally not much technologically skilled.
Any communication on risk must be relevant. Technical information that is too detailed or is sent to inappropriate parties will hinder, rather than enable, a clear view of risk. For each risk, critical moments exist between its origination and its potential business consequence.
Information should also be aimed at the correct target audience and available on need-to-know basis. Hence for effective risk communication risk information should be:
* Clear
* Concise
* Useful
* Timely given
* Aimed at the correct audience
* Available on need-to-know basis

NEW QUESTION: 29
Which of the following terms is described in the statement below?
"They are the prime monitoring indicators of the enterprise, and are highly relevant and possess a high probability of predicting or indicating important risk."
A. Key risk indicators
B. Lag indicators
C. Lead indicators
D. Risk indicators
Answer: (SHOW ANSWER)

Section: Volume C
Explanation:
Key Risk Indicators are the prime monitoring indicators of the enterprise. KRIs are highly relevant and possess a high probability of predicting or indicating important risk. KRIs help in avoiding excessively large number of risk indicators to manage and report that a large enterprise may have.
Incorrect Answers:
B: Lag indicators are the risk indicators that is used to indicate risk after events have occurred.
C: Lead indicators are the risk indicators that is used to indicate which capabilities are in place to prevent events from occurring.
D: Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.

NEW QUESTION: 30
Which of the following is the PRIMARY reason to use key control indicators (KCIs) to evaluate control operating effectiveness?
A. To raise awareness of operational issues
B. To identify control vulnerabilities
C. To measure business exposure to risk
D. To monitor the achievement of set objectives
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 31
Which of the following is the BEST approach to use when creating a comprehensive set of IT risk scenarios?
A. Gather scenarios from senior management
B. Derive scenarios from IT risk policies and standards
C. Benchmark scenarios against industry peers
D. Map scenarios to a recognized risk management framework
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 32
Which section of the Sarbanes-Oxley Act specifies "Periodic financial reports must be certified by CEO and CFO"?
A. Section 302
B. Section 404
C. Section 203
D. Section 409
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Section 302 of the Sarbanes-Oxley Act requires corporate responsibility for financial reports to be certified by CEO, CFO, or designated representative.
Incorrect Answers:
B: Section 404 of the Sarbanes-Oxley Act states that annual assessments of internal controls are the responsibility of management.
C: Section 203 of the Sarbanes-Oxley Act requires audit partners and review partners to rotate off an assignment every five years.
D: Section 409 of the Sarbanes-Oxley Act states that the financial reports must be distributed quickly and currently.

NEW QUESTION: 33
Which of the following parameters are considered for the selection of risk indicators?
Each correct answer represents a part of the solution. Choose three.
A. Size and complexity of the enterprise
B. Type of market in which the enterprise operates
C. Risk appetite and risk tolerance
D. Strategy focus of the enterprise
E. Explanation:
Risk indicators are placed at control points within the enterprise and are used to collect data. These collected data are used to measure the risk levels at that point. They also track events or incidents that may indicate a potentially harmful situation. Risk indicators can be in form of logs, alarms and reports. Risk indicators are selected depending on a number of parameters in the internal and external environment, such as: Size and complexity of the enterprise Type of market in which the enterprise operates Strategy focus of the enterprise
Answer: A,B,D,E (LEAVE A REPLY)
is incorrect. Risk appetite and risk tolerance are considered when applying various risk responses.

NEW QUESTION: 34
You are the project manager of the GHT project. This project will last for 18 months and has a project budget of $567,000. Robert, one of your stakeholders, has introduced a scope change request that will likely have an impact on the project costs and schedule. Robert assures you that he will pay for the extra time and costs associated with the risk event. You have identified that change request may also affect other areas of the project other than just time and cost. What project management component is responsible for evaluating a change request and its impact on all of the project management knowledge areas?
A. Configuration management
B. Integrated change control
C. Risk analysis
D. Project change control system
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Integrated change control is responsible for evaluating a proposed change and determining its impact on all areas of the project: scope, time, cost, quality, human resources, communication, risk, and procurement.
Incorrect Answers:
A: Configuration management defines the management, control, and documentation of the features and functions of the project's product.
C: Risk analysis is not responsible for reviewing the change aspects for the entire project.
D: The project change control system defines the workflow and approval process for proposed changes to the project scope, time, cost, and contracts.

NEW QUESTION: 35
Who should be accountable for ensuring effective cybersecurity controls are established?
A. Security management function
B. Enterprise risk function
C. Risk owner
D. IT management
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 36
Which of the following decision tree nodes have probability attached to their branches?
A. Root node
B. Event node
C. End node
D. Decision node

Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Event nodes represents the possible uncertain outcomes of a risky decision, with at least two nodes to illustrate the positive and negative range of events. Probabilities are always attached to the branches of event nodes.
Incorrect Answers:
A: Root node is the starting node in the decision tree, and it has no branches.
C: End node represents the outcomes of risk and decisions and probability is not attached to it.
D: It represents the choice available to the decision maker, usually between a risky choice and its non- risky counterpart. As it represents only the choices available to the decision makers, hence probability is not attached to it.

NEW QUESTION: 37
Which of the following IS processes provide indirect information?
Each correct answer represents a complete solution. Choose three.
A. Post-implementation reviews of program changes
B. Security log monitoring
C. Problem management
D. Recovery testing
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Security log monitoring, Post-implementation reviews of program changes, and Problem management provide indirect information. Security log monitoring provide indirect information about certain controls in the security environment, particularly when used to analyze the source of failed access attempts.
Post-implementation reviews of program changes provide indirect information about the effectiveness of internal controls over the development process.
Problem management provide indirect information about the effectiveness of several different IS processes that may ultimately be determined to be the source of incidents.
Incorrect Answers:
D: Recovery testing is the direct evidence that the redundancy or backup controls work effectively. It doesn't provide any indirect information.

NEW QUESTION: 38
When defining thresholds for control key performance indicators (KPIs), it is MOST helpful to align:
A. key risk indicators (KRIs) with risk appetite of the business
B. information risk assessments with enterprise risk assessments
C. control performance with risk tolerance of business owners

D. the control key performance indicators (KPIs) with audit findings
Answer: (SHOW ANSWER)

NEW QUESTION: 39
You are using Information system. You have chosen a poor password and also sometimes transmits data over unprotected communication lines. What is this poor quality of password and unsafe transmission refers to?
A. Probabilities
B. Threats
C. Vulnerabilities
D. Impacts
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Vulnerabilities represent characteristics of information resources that may be exploited by a threat. The given scenario describes such a situation, hence it is a vulnerability.
Incorrect Answers:
A: Probabilities represent the likelihood of the occurrence of a threat, and this scenario does not describe a probability.
B: Threats are circumstances or events with the potential to cause harm to information resources. This scenario does not describe a threat.
D: Impacts represent the outcome or result of a threat exploiting a vulnerability. The stem does not describe an impact.

NEW QUESTION: 40
When reviewing management's IT control self-assessments, a risk practitioner noted an ineffective control that links to several low residual risk scenarios. What should be the NEXT course of action?
A. Propose mitigating controls
B. Assess management's risk tolerance
C. Recommend management accept the low risk scenarios
D. Re-evaluate the risk scenarios associated with the control
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 41
Which of the following is the MOST important requirement for monitoring key risk indicators (KRIs) using log analysis?
A. implementing an automated log analysis tool
B. Providing accurate logs m a timely manner
C. Obtaining logs m an easily readable format

D. Collecting logs from the entire set of IT systems
Answer: B (LEAVE A REPLY)

NEW QUESTION: 42
Which of the following is the final step in the policy development process?
A. Management approval
B. Continued awareness activities
C. Communication to employees
D. Maintenance and review
E. Explanation:
Organizations should create a structured ISG document development process. A formal process gives many areas the opportunity to comment on a policy. This is very important for high-level policies that apply to the whole organization. A formal process also makes surethat final policies are communicated to employees. It also provides organizations with a way to make sure that policies are reviewed regularly. In general, a policy development process should include the following steps: In general, a policy development process should include the following steps: 1.Development 2.Stakeholder review 3.Management approval 4.Communication to employees 5.Documentation of compliance or exceptions 6.Continued awareness activities 7.Maintenance and review
Answer: D,E (LEAVE A REPLY)
B, and C are incorrect. These are the earlier phases in policy development process.

NEW QUESTION: 43
Which of the following will MOST improve stakeholders' understanding of the effect of a potential threat?
A. Establishing a risk management committee
B. Updating the organization's risk register to reflect the new threat
C. Establishing metrics to assess the effectiveness of the responses
D. Communicating the results of the threat impact analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 44
An IT control gap has been identified in a key process. Who would be the MOST appropriate owner of the risk associated with this gap?
A. Business process owner
B. Key control owner
C. Operational risk manager
D. Chief information security officer (CISO)
Answer: (SHOW ANSWER)

NEW QUESTION: 45

Which of the following aspects are included in the Internal Environment Framework of COSO ERM?
Each correct answer represents a complete solution. Choose three.
A. Enterprise's integrity and ethical values
B. Enterprise's working environment
C. Enterprise's human resource standards
D. Enterprise's risk appetite
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The internal environment for risk management is the foundational level of the COSO ERM framework, which describes the philosophical basics of managing risks within the implementing enterprise. The different aspects of the internal environment include the enterprise's:
Philosophy on risk management
Risk appetite
Attitudes of Board of Directors
Integrity and ethical values
Commitment to competence
Organizational structure
Authority and responsibility
Human resource standards

NEW QUESTION: 46
Accountability for a particular risk is BEST represented in a:
A. risk register.
B. risk scenario
C. risk catalog
D. RACI matrix.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 47
An organization has outsourced its billing function to an external service provider. Who should own the risk of customer data leakage caused by the service provider?
A. Business process owner
B. Legal counsel
C. The service provider
D. Vendor risk manager
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following do NOT indirect information?
A. Information about the propriety of cutoff
B. Reports that show orders that were rejected for credit limitations.
C. Reports that provide information about any unusual deviations and individual product margins.
D. The lack of any significant differences between perpetual levels and actual levels of goods.
Answer: A (LEAVE A REPLY)
Section: Volume A
Explanation:
Information about the propriety of cutoff is a kind of direct information.
Incorrect Answers:
B: Reports that show orders that were rejected for credit limitations provide indirect information that credit checking aspects of the system are working as intended.
C: Reports that provide information about any unusual deviations and individual product margins (whereby, the price of an item sold is compared to its standard cost) provide indirect information that controls over billing and pricing are operating.
D: The lack of any significant differences between perpetual levels and actual levels provides indirect information that its billing controls are operating.

NEW QUESTION: 49
Which of the following statements is NOT true regarding the risk management plan?
A. The risk management plan is an output of the Plan Risk Management process.
B. The risk management plan is an input to all the remaining risk-planning processes.
C. The risk management plan includes a description of the risk responses and triggers.
D. The risk management plan includes thresholds, scoring and interpretation methods, responsible parties, and budgets.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. The risk management plan does not

include responses to risks or triggers. Responses to risks are documented in the risk register as part of the Plan Risk Responses process.
Incorrect Answers:
A, B, D: These all statements are true for risk management plan. The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. It includes thresholds, scoring and interpretation methods, responsible parties, and budgets. It also acts as input to all the remaining risk-planning processes.

NEW QUESTION: 50
Which of the following is the FIRST step in managing the security risk associated with wearable technology in the workplace?
A. Develop risk awareness training
B. Monitor employee usage
C. Identify the potential risk
D. Assess the potential risk
Answer: (SHOW ANSWER)
Section: Volume D
Explanation/Reference: https://www.isaca.org/Journal/archives/2016/volume-6/Pages/the-dilemma-for-workplace-usage- wearable-technology.aspx

NEW QUESTION: 51
Which of the following is MOST important to communicate to senior management during the initial implementation of a risk management program?
A. Desired risk level
B. Risk ownership
C. Regulatory compliance
D. Best practices
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
Jeff works as a Project Manager for www.company.com Inc. He and his team members are involved in the identify risk process. Which of the following tools & techniques will Jeff use in the identify risk process?
Each correct answer represents a complete solution. Choose all that apply.
A. Information gathering technique
B. Documentation reviews
C. Checklist analysis
D. Risk categorization
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:

Explanation:
The various tools & techniques used in the identify risk process are as follows:
Documentation reviews
- Information gathering technique
- Checklist analysis
- Assumption analysis
- Diagramming techniques
- SWOT analysis
- Expert judgment

NEW QUESTION: 53
Which of the following is the best reason for performing risk assessment?
A. To determine the present state of risk
B. To analyze the effect on the business
C. To satisfy regulatory requirements
D. To budget appropriately for the application of various controls
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risk assessment is a process of analyzing the identified risk, both quantitatively and qualitatively. Quantitative risk assessment requires calculations of two components of risk, the magnitude of the potential loss, and the probability that the loss will occur. While qualitatively risk assessment checks the severity of risk. Hence risk assessment helps in determining the present state of the risk.
Incorrect Answers:
B: Analyzing the effect of risk on an enterprise is the part of the process while performing risk assessment, but is not the reason for doing it.
C: Performing risk assessment may satisfy the regulatory requirements, but is not the reason to perform risk assessment.
D: Budgeting appropriately is one the results of risk assessment but is not the reason for performing the risk assessment.

NEW QUESTION: 54
John is the project manager of the NHQ Project for his company. His project has 75 stakeholders, some of which are external to the organization. John needs to make certain that he communicates about risk in the most appropriate method for the external stakeholders. Which project management plan will be the best guide for John to communicate to the external stakeholders?
A. Risk Response Plan

B. Communications Management Plan
C. Project Management Plan
D. Risk Management Plan
Answer: (SHOW ANSWER)
Section: Volume D
Explanation
Explanation:
The Communications Management Plan will direct John on the information to be communicated, when to communicate, and how to communicate with external stakeholders.
The Communications Management Plan aims to define the communication necessities for the project and how the information will be circulated. The Communications Management Plan sets the communication structure for the project. This structure provides guidance for communication throughout the project's life and is updated as communication needs change. The Communication Managements Plan identifies and defines the roles of persons concerned with the project. It includes a matrix known as the communication matrix to map the communication requirements of the project.
Incorrect Answers:
A: The Risk Response Plan identifies how risks will be responded to.
C: The Project Management Plan is the parent of all subsidiary management plans and it is not the most accurate choice for this question D: The Risk Management Plan defines how risks will be identified, analyzed, responded to, and controlled throughout the project.

NEW QUESTION: 55
Days before the realization of an acquisition, a data breach is discovered at the company to be acquired. For the accruing organization, this situation represents which of the following?
A. Inherent risk
B. Security incident
C. Risk event
D. Threat event
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following parameters are considered for the selection of risk indicators?
Each correct answer represents a part of the solution. Choose three.
A. Size and complexity of the enterprise
B. Type of market in which the enterprise operates
C. Risk appetite and risk tolerance
D. Strategy focus of the enterprise
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

Risk indicators are placed at control points within the enterprise and are used to collect data. These collected data are used to measure the risk levels at that point. They also track events or incidents that may indicate a potentially harmful situation.
Risk indicators can be in form of logs, alarms and reports. Risk indicators are selected depending on a number of parameters in the internal and external environment, such as:
Size and complexity of the enterprise
- Type of market in which the enterprise operates
- Strategy focus of the enterprise

Incorrect Answers:
C: Risk appetite and risk tolerance are considered when applying various risk responses.

NEW QUESTION: 57
An external security audit has reported multiple findings related to control noncompliance. Which of the following would be MOST important for the risk practitioner to communicate to senior management?
A. Plans for mitigating the associated risk
B. Suggestions for improving risk awareness training
C. A recommendation for internal audit validation
D. The impact to the organization's risk profile
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 58
An organization is considering allowing users to access company data from their personal devices. Which of the following is the MOST important factor when assessing the risk?
A. Classification of the data
B. Type of device
C. Remote management capabilities
D. Volume of data
Answer: C (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 59
During a control review, the control owner states that an existing control has deteriorated over time. What is the BEST recommendation to the control owner?
A. Implement compensating controls to reduce residual risk
B. Certify the control after documenting the concern.
C. Escalate the issue to senior management
D. Discuss risk mitigation options with the risk owner.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 60
When evaluating enterprise IT risk management it is MOST important to:
A. create new control processes to reduce identified IT risk scenarios
B. report identified IT risk scenarios to senior management
C. review alignment with the organization's investment plan
D. confirm the organization s risk appetite and tolerance
Answer: (SHOW ANSWER)

NEW QUESTION: 61
You are the risk professional in Bluewell Inc. A risk is identified and enterprise wants to quickly implement control by applying technical solution that deviates from the company's policies. What you should do?
A. Recommend against implementation because it violates the company's policies
B. Recommend revision of the current policy
C. Recommend a risk assessment and subsequent implementation only if residual risk is accepted
D. Conduct a risk assessment and allow or disallow based on the outcome
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
If it is necessary to quickly implement control by applying technical solution that deviates from the company's policies, then risk assessment should be conducted to clarify the risk. It is up to the management to accept the risk or to mitigate it.
Incorrect Answers:
A: As in this case it is important to mitigate the risk, hence risk professional should once recommend a risk assessment. Though the decision for the conduction of risk assessment in case of violation of company's policy, is taken by management.
B: The recommendation to revise the current policy should not be triggered by a single request.
D: Risk professional can only recommend the risk assessment if the company's policies is violating, but it can only be conducted when the management allows.

NEW QUESTION: 62
During which of the following processes, probability and impact matrix are prepared?
A. Risk response
B. Monitoring and Control Risk
C. Quantitative risk assessment
D. Qualitative risk assessment
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation
Explanation:
The probability and impact matrix is a technique to prioritize identified risks of the project on their risk rating, and are being prepared while performing qualitative risk analysis. Evaluation of each risk's importance and, hence, priority for attention, is typically conducted using a look-up table or a probability and impact matrix. This matrix specifies combinations of probability and impact that lead to rating the risks as low, moderate, or high priority.
Incorrect Answers:
A, B: These processes are part of Risk Management. The probability and impact matrix is prepared during the qualitative risk analysis for further quantitative analysis and response based on their risk rating.
C: SLE, ARO and ALE are used in quantitative risk assessment.

NEW QUESTION: 63
Which of the following is the greatest risk to reporting?
A. Integrity of data
B. Availability of data
C. Confidentiality of data
D. Reliability of data
E. Explanation:
Reporting risks are caused due to wrong reporting which leads to bad decision. This bad decision due to wrong report hence causes a risk on the functionality of the organization. Therefore, the greatest risk to reporting is reliability of data. Reliability of data refers to the accuracy, robustness, and timing of the data.
Answer: (SHOW ANSWER)
B, and C are incorrect. Integrity, availability, and confidentiality of data are also important, but these three in combination comes under reliability itself.

NEW QUESTION: 64

Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?

A. Review the risk register and risk scenarios

B. Calculate annualized loss expectancy of risk scenarios

C. Raise the maturity of organizational risk management

D. Perform a return on investment analysis

Answer: B (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 65

Which of the following will BEST support management reporting on risk?

A. A risk register.

B. Key performance indicators.

C. Control self-assessment.

D. Risk policy requirements.

Answer: B (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 66

An application runs a scheduled job that compiles financial data from multiple business systems and updates the financial reporting system. If this job runs too long, it can delay financial reporting. Which of the following is the risk practitioner's BEST recommendation?

A. Implement database activity and capacity monitoring.

B. Consider providing additional system resource to this job.

C. Ensure the enterprise has a process to detect such situations.

D. Ensure the business is aware of the risk.

Answer: C (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 67

Mary is a project manager in her organization. On her current project she is working with her project team and other key stakeholders to identify the risks within the project. She is currently aiming to create a comprehensive list of project risks so she is using a facilitator to help generate ideas about project risks. What risk identification method is Mary likely using?

A. Delphi Techniques

B. Expert judgment

C. Brainstorming

D. Checklist analysis

Answer: (SHOW ANSWER)

Section: Volume A

Explanation:
Mary is using brainstorming in this example. Brainstorming attempts to create a comprehensive list of risks and often is led by a moderator or facilitator to move the process along.
Brainstorming is a technique to gather general data. It can be used to identify risks, ideas, or solutions to issues by using a group of team members or subject-matter expert. Brainstorming is a group creativity technique that also provides other benefits, such as boosting morale, enhancing work enjoyment, and improving team work.
Incorrect Answers:
A: The Delphi technique uses rounds of anonymous surveys to generate a consensus on the identified risks.
B: Expert judgment is not the best answer for this; projects experts generally do the risk identification, in addition to the project team.
D: Checklist analysis uses historical information and information from similar projects within the organization's experience.

NEW QUESTION: 68
A PRIMARY function of the risk register is to provide supporting information for the development of an organization's risk:
A. profile.
B. process.
C. map.
D. strategy.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
Which of the following should be determined FIRST when a new security vulnerability is made public?
A. What mitigating controls are currently in place
B. Whether the affected technology is used within the organization
C. How pervasive the vulnerability is within the organization
D. Whether the affected technology is Internet-facing
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following is the BEST method of creating risk awareness in an organization?
A. Appointing the risk manager from the business units
B. Ensuring senior management commitment to risk training
C. Marking the risk register available to project stakeholders
D. Providing regular communication to risk managers
Answer: B (LEAVE A REPLY)

NEW QUESTION: 71
Which of the following is the BEST indication of the effectiveness of a business continuity program?
A. Business impact analyses are reviewed and updated in a timely manner.
B. Business units are familiar with the business continuity plans and process.
C. Business continuity tests are performed successfully and issues are addressed.
D. Business continuity and disaster recovery plans are regularly updated.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
Which of the following is the BEST defense against successful phishing attacks?
A. Intrusion detection system
B. Application hardening
C. End-user awareness
D. Spam filters
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing attacks are a type of to social engineering attack and are best defended by end-user awareness training.
Incorrect Answers:
A: An intrusion detection system does not protect against phishing attacks since phishing attacks usually do not have a particular pattern or unique signature.
B: Application hardening does not protect against phishing attacks since phishing attacks generally use e- mail as the attack vector, with the end-user as the vulnerable point, not the application.
D: Certain highly specialized spam filters can reduce the number of phishing e-mails that reach the inboxes of user, but they are not as effective in addressing phishing attack as end-user awareness.

NEW QUESTION: 73
Which of the following MUST be updated to maintain an IT risk register?
A. Risk tolerance
B. Enterprise-wide IT risk assessment
C. Risk appetite
D. Expected frequency and potential impact
Answer: D (LEAVE A REPLY)

NEW QUESTION: 74

Which of the following stakeholders are typically included as part of a line of defense within the three lines of defense model?
A. Legal team
B. Board of directors
C. Vendors
D. Regulators
Answer: (SHOW ANSWER)

NEW QUESTION: 75
A risk practitioner shares the results of a vulnerability assessment for a critical business application with the business manager. Which of the following is the NEXT step?
A. Conduct a penetration test to validate the vulnerabilities from the findings.
B. Evaluate the impact of the vulnerabilities to the business application.
C. Develop a risk action plan to address the findings.
D. Escalate the findings to senior management and internal audit.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 76
Which of the following is MOST critical when designing controls?
A. Involvement of process owner
B. Quantitative impact of the risk
C. Involvement of internal audit
D. Identification of key risk indicators
Answer: A (LEAVE A REPLY)

NEW QUESTION: 77
Which of the following is the MOST important consideration when developing an organization's risk taxonomy?
A. Regulatory requirements
B. Business context
C. Leading industry frameworks
D. IT strategy

Answer: A (LEAVE A REPLY)

NEW QUESTION: 78
You are the project manager in your enterprise. You have identified occurrence of risk event in your enterprise. You have pre-planned risk responses. You have monitored the risks that had occurred. What is the immediate step after this monitoring process that has to be followed in response to risk events?
A. Initiate incident response
B. Update the risk register
C. Eliminate the risk completely
D. Communicate lessons learned from risk events
Answer: A (LEAVE A REPLY)
When the risk events occur then following tasks have to done to react to it: Maintain incident response plans Monitor risk Initiate incident response Communicate lessons learned from risk events

NEW QUESTION: 79
You have been assigned as the Project Manager for a new project that involves development of a new interface for your existing time management system. You have completed identifying all possible risks along with the stakeholders and team and have calculated the probability and impact of these risks. Which of the following would you need next to help you prioritize the risks?
A. Affinity Diagram
B. Risk rating rules
C. Project Network Diagram
D. Risk categories
Answer: B (LEAVE A REPLY)
Section: Volume A
Explanation:
Risk rating rules define how to prioritize risks after the related probability and impact values are calculated.
These are generally included in the organizational process assets and are refined for individual projects.
Incorrect Answers:
A: Affinity Diagram is a method of group creativity technique to collect requirements which allows large numbers of ideas to be sorted into groups for review and analysis. This is generally used in Scope Management and not applicable to this option.
C: A Project Network diagram shows the sequencing and linkage between various project tasks and is not applicable to this question D: Risk categories are an output of the Perform Qualitative Risk Analysis process and not a tool to complete the process.

NEW QUESTION: 80

An organization is increasingly concerned about loss of sensitive data and asks the risk practitioner to assess the current risk level. Which of the following should the risk practitioner do FIRST?

A. Identify staff members who have access to the organization's sensitive data.

B. Identify risk scenarios and owners associated with possible data loss vectors.

C. Identify locations where the organization's sensitive data is stored.

D. Identify existing data loss controls and their levels of effectiveness.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 81

After the implementation of Internet of Things (IoT) devices, new risk scenarios were identified. What is the PRIMARY reason to report this information to risk owners?

A. To reevaluate continued use of IoT devices.

B. To recommend changes to the IoT policy.

C. To confirm the impact to the risk profile.

D. To add new controls to mitigate the risk.

Answer: D (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 82

Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?

A. Regularly scheduled audits

B. Incident reporting procedures

C. Incident management policy

D. Organizational reporting process

Answer: D (LEAVE A REPLY)

NEW QUESTION: 83

Key risk indicators (KRIs) are MOST useful during which of the following risk management phases?

A. Analysis

B. Monitoring

C. Response selection

D. Identification

Answer: (SHOW ANSWER)

NEW QUESTION: 84

Which of the following should an organization perform to forecast the effects of a disaster?

A. Analyze capability maturity model gaps.

B. Define recovery time objectives (RTO).

C. Develop a business impact analysis (BIA).
D. Simulate a disaster recovery.
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 85
To communicate the risk associated with IT in business terms, which of the following MUST be defined?
A. Risk appetite of the organization
B. Inherent and residual risk
C. Compliance objectives
D. Organizational objectives
Answer: B (LEAVE A REPLY)

NEW QUESTION: 86
You are the project manager of a HGT project that has recently finished the final compilation process. The project customer has signed off on the project completion and you have to do few administrative closure activities. In the project, there were several large risks that could have wrecked the project but you and your project team found some new methods to resolve the risks without affecting the project costs or project completion date. What should you do with the risk responses that you have identified during the project's monitoring and controlling process?
A. Include the responses in the project management plan.
B. Include the risk responses in the risk management plan.
C. Include the risk responses in the organization's lessons learned database.
D. Nothing. The risk responses are included in the project's risk register already.
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:
The risk responses that do not exist up till then, should be included in the organization's lessons learned database so other project managers can use these responses in their project if relevant.
Incorrect Answers:
A: The responses are not in the project management plan, but in the risk response plan during the project and they'll be entered into the organization's lessons learned database.
B: The risk responses are included in the risk response plan, but after completing the project, they should be entered into the organization's lessons learned database.
D: If the new responses that were identified is only included in the project's risk register then it may not be shared with project managers working on some other project.

NEW QUESTION: 87

You are the project manager of the NHH Project. You are working with the project team to create a plan to document the procedures to manage risks throughout the project. This document will define how risks will be identified and quantified. It will also define how contingency plans will be implemented by the project team. What document do you and your team is creating in this scenario?

A. Project plan

B. Resource management plan

C. Project management plan

D. Risk management plan

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The risk management plan, part of the comprehensive management plan, defines how risks will be identified, analyzed, monitored and controlled, and even responded to.

A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.

Risks are built in with any project, and project managers evaluate risks repeatedly and build plans to address them. The risk management plan consists of analysis of possible risks with both high and low impacts, and the mitigation strategies to facilitate the project and avoid being derailed through which the common problems arise. Risk management plans should be timely reviewed by the project team in order to avoid having the analysis become stale and not reflective of actual potential project risks. Most critically, risk management plans include a risk strategy for project execution.

Incorrect Answers:

A: The project plan is not an official PMBOK project management plan.

B: The resource management plan defines the management of project resources, such as project team members, facilities, equipment, and contractors.

C: The project management plan is a comprehensive plan that communicates the intent of the project for all project management knowledge areas.

NEW QUESTION: 88

An IT risk practitioner has determined that mitigation activities differ from an approved risk action plan. Which of the following is the risk practitioner's BEST course of action?

A. Revert the implemented mitigation measures until approval is obtained

B. Update the risk register with the implemented risk mitigation actions.

C. Validate the adequacy of the implemented risk mitigation measures.

D. Report the observation to the chief risk officer (CRO).

Answer: (SHOW ANSWER)

NEW QUESTION: 89

Which of the following would be an IT business owner's BEST course of action following an unexpected increase in emergency changes?
A. Conducting a root-cause analysis
B. Validating the adequacy of current processes
C. Evaluating the impact to control objectives
D. Reconfiguring the IT infrastructure
Answer: (SHOW ANSWER)
Section: Volume D
Explanation

NEW QUESTION: 90
There are four inputs to the Monitoring and Controlling Project Risks process. Which one of the following will NOT help you, the project manager, to prepare for risk monitoring and controlling?
A. Risk register
B. Work Performance Information
C. Project management plan
D. Change requests
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Change requests are not one of the four inputs to the Risk Monitoring and Controlling Process. The four inputs are the risk register, the project management plan, work performance information, and performance reports.
Incorrect Answers:
A, B, C: These are the valid inputs to the Risk Monitoring and Controlling Process.

NEW QUESTION: 91
Which of the following is the PRIMARY purpose of periodically reviewing an organization's risk profile?
A. Update risk responses in the risk register
B. Design and implement risk response action plans.
C. Altgn business objectives with risk appetite.
D. Enable risk-based decision making.
Answer: (SHOW ANSWER)

NEW QUESTION: 92
Marie has identified a risk event in her project that needs a mitigation response. Her response actually creates a new risk event that must now be analyzed and planned for. What term is given to this newly created risk event?
A. Residual risk
B. Secondary risk
C. Infinitive risk
D. Populated risk
Answer: B (LEAVE A REPLY)
Section: Volume B
Explanation
Explanation:
Secondary risks are the risks that come about as a result of implementing a risk response. This new risk event must be recorded, analyzed, and planned for management.
Incorrect Answers:
A: A residual risk event is similar to a secondary risk, but is often small in probability and impact, so it may just be accepted.
C: Infinitive risk is not a valid project management term.
D: Populated risk event is not a valid project management term.

NEW QUESTION: 93
A change management process has recently been updated with new testing procedures. The NEXT course of action is to:
A. communicate to those who test and promote changes
B. assess the maturity of the change management process
C. conduct a cost-benefit analysis to justify the cost of the control
D. monitor processes to ensure recent updates are being followed
Answer: (SHOW ANSWER)
Section: Volume D
Explanation

NEW QUESTION: 94
Which of the following BEST measures the efficiency of an incident response process?
A. Average time between changes and updating of escalation matrix
B. Average gap between actual and agreed response times
C. Number of incidents lacking responses
D. Number of incidents escalated to management
Answer: (SHOW ANSWER)

NEW QUESTION: 95
An organization wants to assess the maturity of its internal control environment. The FIRST step should be to:
A. validate control process execution.
B. determine if controls are effective.
C. conduct a baseline assessment.
D. identify key process owners.
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Following a significant change to a business process, a risk practitioner believes the associated risk has been reduced. The risk practitioner should advise the risk owner to FIRST
A. review the key risk indicators.
B. reallocate risk response resources.
C. update the risk register
D. conduct a risk analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 97
Which of the following is the BEST way to confirm whether appropriate automated controls are in place within a recently implemented system?
A. Conduct user acceptance testing
B. Perform a post-implementation review
C. Interview process owners
D. Review the key performance indicators (KPIs)
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 98
Which of the following vulnerability assessment software can check for weak passwords on the network?
A. Password cracker
B. Antivirus software
C. Anti-spyware software
D. Wireshark
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A password cracker is an application program that is used to identify an unknown or forgotten password on a computer or network resources. It can also be used to help a human cracker

obtain unauthorized access to resources. A password cracker can also check for weak passwords on the network and give notifications to put another password.
Incorrect Answers:
B: Antivirus or anti-virus software is used to prevent, detect, and remove malware. It scans the computer for viruses.
C: Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.
D: Wireshark is a free and open-source protocol analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NEW QUESTION: 99
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?
A. Sufficient resources are not assigned to IT development projects.
B. The corporate email system does not identify and store phishing emails.
C. Email infrastructure does not have proper rollback plans.
D. Customer support help desk staff does not have adequate training.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
An organization has used generic risk scenarios to populate its risk register. Which of the following presents the GREATEST challenge to assigning of the associated risk entries?
A. Risk aggregation has not been completed
B. Risk scenarios are not applicable
C. The risk analysts for each scenario is incomplete
D. The volume of risk scenarios is too large
Answer: B (LEAVE A REPLY)

NEW QUESTION: 101
If preventive controls cannot be implemented due to technology limitations, which of the following should be done FIRST to reduce risk?
A. Redefine the business process to reduce the risk
B. Evaluate alternative controls
C. Develop a plan to upgrade technology
D. Define a process for monitoring risk
Answer: (SHOW ANSWER)
Section: Volume D
Explanation

NEW QUESTION: 102

A key risk indicator (KRI) threshold has reached the alert level, indicating data leakage incidents are highly probable. What should be the risk practitioner's FIRST course of action?
A. Perform a root cause analysis.
B. Update the KRI threshold.
C. Review incident handling procedures.
D. Recommend additional controls.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 103
Which among the following is the BEST reason for defining a risk response?
A. To eliminate risk from the enterprise
B. To ensure that the residual risk is within the limits of the risk appetite and tolerance
C. To overview current status of risk
D. To mitigate risk
Answer: B (LEAVE A REPLY)
Section: Volume C
Explanation:
The purpose of defining a risk response is to ensure that the residual risk is within the limits of the risk appetite and tolerance of the enterprise. Risk response is based on selecting the correct, prioritized response to risk, based on the level of risk, the enterprise's risk tolerance and the cost or benefit of the particular risk response option.
Incorrect Answers:
A: Risk cannot be completely eliminated from the enterprise.
C: This is not a valid answer.
D: Mitigation of risk is itself the risk response process, not the reason behind this.

NEW QUESTION: 104
Which of the following IT controls is MOST useful in mitigating the risk associated with inaccurate data?
A. Check totals on data records and data fields
B. Links to source data
C. Audit trails for updates and deletions
D. Encrypted storage of data
Answer: (SHOW ANSWER)

NEW QUESTION: 105
Which of the following vulnerability assessment software can check for weak passwords on the network?
A. Password cracker
B. Antivirus software
C. Anti-spyware software

D. Wireshark
Answer: A (LEAVE A REPLY)
Section: Volume B
Explanation:
A password cracker is an application program that is used to identify an unknown or forgotten password on a computer or network resources. It can also be used to help a human cracker obtain unauthorized access to resources. A password cracker can also check for weak passwords on the network and give notifications to put another password.
Incorrect Answers:
B: Antivirus or anti-virus software is used to prevent, detect, and remove malware. It scans the computer for viruses.
C: Anti-spyware software is a type of program designed to prevent and detect unwanted spyware program installations and to remove those programs if installed.
D: Wireshark is a free and open-source protocol analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NEW QUESTION: 106
A PRIMARY advantage of involving business management in evaluating and managing risk is that management:
A. better understands the system architecture
B. can balance technical and business risk
C. can make better informed business decisions
D. is more objective than risk management
Answer: C (LEAVE A REPLY)

NEW QUESTION: 107
You are the project manager of GHT project. Your hardware vendor left you a voicemail saying that the delivery of the equipment you have ordered would not arrive on time. She wanted to give you a heads-up and asked that you return the call. Which of the following statements is TRUE?
A. This is a residual risk.
B. This is a trigger.
C. This is a contingency plan.

D. This is a secondary risk.
E. Explanation:
Triggers are warning signs of an upcoming risk event. Here delay in delivery signifies that there may be a risk event like delay in completion of project. Hence it is referred to as a trigger.
F. is incorrect. A contingency plan is a plan devised for a specific situation when things go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen.
Here there are no such plans.
G. is incorrect. Residual risk is the risk that remains after applying controls. But here in this scenario, risk event has not occurred yet.
Answer: B (LEAVE A REPLY)
is incorrect. Secondary risks are risks that come about as a result of implementing a risk response. But here in this scenario, risk event has not occurred yet.

NEW QUESTION: 108
Which type of indicators should be developed to measure the effectiveness of an organization's firewall rule set?
A. Key risk indicators (KRIs)
B. Key control indicators (KCIs)
C. Key management indicators (KMIs)
D. Key performance indicators (KPIs)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 109
Which of the following is the way to verify control effectiveness?
A. The capability of providing notification of failure.
B. Whether it is preventive or detective.
C. Its reliability.
D. The test results of intended objectives.
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Control effectiveness requires a process to verify that the control process worked as intended and meets the intended control objectives.
Hence the test result of intended objective helps in verifying effectiveness of control.
Incorrect Answers:
A: Notification of failure does not determine control strength, hence this option is not correct.
B: The type of control, like preventive or detective, does not help determine control effectiveness.
C: Reliability is not an indication of control strength; weak controls can be highly reliable, even if they do not meet the control objective.

NEW QUESTION: 110
An organization has completed a risk assessment of one of its service providers. Who should be accountable for ensuring that risk responses are implemented?
A. IT risk practitioner
B. Legal representation of the business
C. The relationship owner
D. Third -partf3ecurity team
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
Which of the following would BEST help secure online financial transactions from improper users?
A. Multi-factor authentication
B. Periodic review of audit trails
C. Multi-level authorization
D. Review of log-in attempts
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 112
An organization has experienced several incidents of extended network outages that have exceeded tolerance. Which of the following should be the risk practitioner's FIRST step to address this situation?
A. Recommend a root cause analysis of the incidents.
B. Update the incident-related risk trend in the risk register.
C. Recommend additional controls to address the risk.
D. Update the risk tolerance level to acceptable thresholds.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 113
Which of the following should be the PRIMARY consideration when assessing the automation of control monitoring?
A. Cost-benefit analysis of automation
B. Frequency of failure of control
C. impact due to failure of control
D. Contingency plan for residual risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114

You are the project manager of HWD project. It requires installation of some electrical machines. You and the project team decided to hire an electrician as electrical work can be too dangerous to perform. What type of risk response are you following?

A. Avoidance

B. Transference

C. Mitigation

D. Acceptance

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

As the risk is transferred to the third party (electrician), hence this type of risk response is transference.

Incorrect Answers:

A: Risk avoidance means to evade risk altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event. Risk avoidance is applied when the level of risk, even after the applying controls, would be greater than the risk tolerance level of the enterprise.

C: Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level.

Risk mitigation can utilize various forms of control carefully integrated together.

D: Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs.

NEW QUESTION: 115

Which of the following actions assures management that the organization's objectives are protected from the occurrence of risk events?

A. Internal control

B. Risk management

C. Hedging

D. Risk assessment

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Internal controls are the actions taken by the organization to help to assure management that the organization's objectives are protected from the occurrence of risk events. Internal control objectives are applicable to all manual or automated areas. Internal control objectives include:

Internal accounting controls- They control accounting operations, including safeguarding assets and

- financial records.

Operational controls- They focus on day-to-day operations, functions, and activities. They ensure that

- all the organization's objectives are being accomplished.

Administrative controls- They focus on operational efficiency in a functional area and stick to

- management policies.

Incorrect Answers:

B: Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources. It is done to minimize, monitor, and control the probability and impact of unfortunate events or to maximize the realization of opportunities.

C: Hedging is the process of managing the risk of price changes in physical material by offsetting that risk in the futures market. In other words, it is the avoidance of risk. So, it only avoids risk but can not assure protection against risk.

D: Risk assessment is a process of analyzing the identified risk, both quantitatively and qualitatively.

Quantitative risk assessment requires calculations of two components of risk, the magnitude of the potential loss, and the probability that the loss will occur. While qualitatively risk assessment checks the severity of risk. The assessment attempts to determine the likelihood of the risk being realized and the impact of the risk on the operation. This provides several conclusions:

Probability-establishing the likelihood of occurrence and reoccurrence of specific risks, independently

- and combined.

Interdependencies-the relationship between different types of risk. For instance, one risk may have

- greater potential of occurring if another risk has occurred. Or probability or impact of a situation may increase with combined risk.

NEW QUESTION: 116

After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:

After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:

Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

A. Regulatory examination

B. Vendor performance scorecard

C. External audit
D. Internal audit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
You have been assigned as the Project Manager for a new project that involves development of a new interface for your existing time management system. You have completed identifying all possible risks along with the stakeholders and team and have calculated the probability and impact of these risks. Which of the following would you need next to help you prioritize the risks?
A. Affinity Diagram
B. Risk rating rules
C. Project Network Diagram
D. Risk categories
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risk rating rules define how to prioritize risks after the related probability and impact values are calculated.
These are generally included in the organizational process assets and are refined for individual projects.
Incorrect Answers:
A: Affinity Diagram is a method of group creativity technique to collect requirements which allows large numbers of ideas to be sorted into groups for review and analysis. This is generally used in Scope Management and not applicable to this option.
C: A Project Network diagram shows the sequencing and linkage between various project tasks and is not applicable to this question D: Risk categories are an output of the Perform Qualitative Risk Analysis process and not a tool to complete the process.

NEW QUESTION: 118
Which of the following processes is described in the statement below?
"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."
A. Perform Quantitative Risk Analysis
B. Monitor and Control Risks
C. Identify Risks
D. Perform Qualitative Risk Analysis
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:

Monitor and Control Risk is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project. It can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project management plan.
Incorrect Answers:
B: This is the process of numerically analyzing the effect of identified risks on overall project objectives.
C: This is the process of determining which risks may affect the project and documenting their characteristics.
D: This is the process of prioritizing risks for further analysis or action by accessing and combining their probability of occurrence and impact.

NEW QUESTION: 119
An organization delegates its data processing to the internal IT team to manage information through its applications. Which of the following is the role of the internal IT team in this situation?
A. Data custodians
B. Data processors
C. Data owners
D. Data controllers
Answer: (SHOW ANSWER)

NEW QUESTION: 120
A maturity model is MOST useful to an organization when it:
A. defines a qualitative measure of risk
B. provides risk metrics.
C. benchmarks against other organizations
D. provides a reference for progress
Answer: (SHOW ANSWER)

NEW QUESTION: 121
Which of the following IT key risk indicators (KRIs) provides management with the BEST feedback on IT capacity?
A. Trends in IT resource usage.
B. Increased resource availability.
C. Trends in IT maintenance costs.
D. Increased number of incidents.
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 122
Which of the following is the BEST key performance indicator (KPI) to measure the ability to deliver uninterrupted IT services?
A. Mean time between failures
B. Unplanned downtime
C. Mean time to recover
D. Planned downtime
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 123
John works as a project manager for BlueWell Inc. He is determining which risks can affect the project.
Which of the following inputs of the identify risks process is useful in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk?
A. Activity duration estimates
B. Activity cost estimates
C. Risk management plan
D. Schedule management plan
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The activity duration estimates review is valuable in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk.
Incorrect Answers:
B: The activity cost estimates review is valuable in identifying risks as it provides a quantitative assessment of the expected cost to complete scheduled activities and is expressed as a range, with a width of the range indicating the degrees of risk.
C: A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.

D: It describes how the schedule contingencies will be reported and assessed.

NEW QUESTION: 124
To reduce the risk introduced when conducting penetration tests, the BEST mitigating control would be to:
A. notify network administrators before testing
B. clearly define the project scope.
C. perform background checks on the vendor.
D. require the vendor to sign a nondisclosure agreement
Answer: (SHOW ANSWER)

NEW QUESTION: 125
Which of the following would BEST help minimize the risk associated with social engineering threats?
A. Reviewing the organization's risk appetite
B. Enforcing employee sanctions
C. Enforcing segregation of duties
D. Conducting phishing exercises
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 126
What is the IMMEDIATE step after defining set of risk scenarios?
A. Risk mitigation
B. Risk monitoring
C. Risk management
D. Risk analysis
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, likelihood and impact of the scenarios are assessed. Important components of this assessment are the risk factors.
Incorrect Answers:
A: Risk mitigation is the latter step after analyzing risk.
B: Risk monitoring is the latter step after risk analysis and risk mitigation.
C: Risk analysis comes under risk management, therefore management is a generalized term, and is not the best answer for this question.

NEW QUESTION: 127

Which of the following observations would be GREATEST concern to a risk practitioner reviewing the implementation status of management action plans?
A. Management has not begun the implementation.
B. Management has not determined a final implementation date.
C. Management has not secured resources for mitigation activities.
D. Management has not completed an early mitigation milestone.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
Henry is the project sponsor of the JQ Project and Nancy is the project manager. Henry has asked Nancy to start the risk identification process for the project, but Nancy insists that the project team be involved in the process. Why should the project team be involved in the risk identification?
A. So that the project team can develop a sense of ownership for the risks and associated risk responsibilities.
B. So that the project manager can identify the risk owners for the risks within the project and the needed risk responses.
C. So that the project manager isn't the only person identifying the risk events within the project.
D. So that the project team and the project manager can work together to assign risk ownership.
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The best answer to include the project team members is that they'll need to develop a sense of ownership for the risks and associated risk responsibilities.
Incorrect Answers:
B: The reason to include the project team is that the project team needs to develop a sense of ownership for the risks and associated risk responsibilities, not to assign risk ownership and risk responses at this point.
C: While the project manager shouldn't be the only person to identify the risk events, this isn't the best answer.
D: The reason to include the project team is that the project team needs to develop a sense of ownership for the risks and associated risk responsibilities, not to assign risk ownership.

NEW QUESTION: 129
You are the project manager of RFT project. You have identified a risk that the enterprise's IT system and application landscape is so complex that, within a few years, extending capacity will become difficult and maintaining software will become very expensive. To overcome this risk, the response adopted is re- architecture of the existing system and purchase of new integrated system. In which of the following risk prioritization options would this case be categorized?
A. Deferrals
B. Quick win

C. Business case to be made
D. Contagious risk
Answer: (SHOW ANSWER)
Section: Volume C
Explanation/Reference:
Explanation:
This is categorized as a Business case to be made because the project cost is very large. The response to be implemented requires quite large investment. Therefore it comes under business case to be made.
Incorrect Answers:
A: It addresses costly risk response to a low risk. But here the response is less costly than that of business case to be made.
B: Quick win is very effective and efficient response that addresses medium to high risk. But in this the response does not require large investments.
D: This is not risk response prioritization option, instead it is a type of risk that happen with the several of the enterprise's business partners within a very short time frame.

NEW QUESTION: 130
Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?
A. Organizational reporting process.
B. Incident reporting procedures.
C. Regularly scheduled audits.
D. Incident management policy.
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 131
What are the requirements for creating risk scenarios? Each correct answer represents a part of the solution.
Choose three.
A. Determination of cause and effect
B. Determination of the value of business process at risk
C. Potential threats and vulnerabilities that could cause loss
D. Determination of the value of an asset
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:

Creating a scenario requires determination of the value of an asset or a business process at risk and the potential threats and vulnerabilities that could cause loss. The risk scenario should be assessed for relevance and realism, and then entered into the risk register if found to be relevant. In practice following steps are involved in risk scenario development:
* First determine manageable set of scenarios, which include:
- Frequently occurring scenarios in the industry or product area.
- Scenarios representing threat sources that are increasing in count or severity level.
- Scenarios involving legal and regulatory requirements applicable to the business.
* After determining manageable risk scenarios, perform a validation against the business objectives of the entity.
* Based on this validation, refine the selected scenarios and then detail them to a level in line with the criticality of the entity.
* Lower down the number of scenarios to a manageable set. Manageable does not signify a fixed number, but should be in line with the overall importance and criticality of the unit.
* Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
* Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
* Include an unspecified event in the scenarios, that is, address an incident not covered by other scenarios.
Incorrect Answers:
A: Cause-and-effect analysis is a predictive or diagnostic analytical tool used to explore the root causes or factors that contribute to positive or negative effects or outcomes. It is used during the process of exposing risk factors.

NEW QUESTION: 132
What are the various outputs of risk response?
A. Risk Priority Number
B. Residual risk
C. Risk register updates
D. Project management plan and Project document updates
E. Risk-related contract decisions
F. Explanation:
The outputs of the risk response planning process are: Risk Register Updates: The risk register is written in detail so that it can be related to the priority ranking and the planned response. Risk Related Contract Decisions: Risk related contract decisions are the decisions to transmit risk, such as services, agreements for insurance, and other items as required. It provides a means for sharing risks. Project Management Plan Updates: Some of the elements of the project management plan updates are: Schedule management plan Cost management plan Quality management plan Procurement management plan Human resource management plan Work breakdown structure Schedule baseline Cost performance baseline Project Document Updates:

Some of the project documents that can be updated includes: Assumption log updates Technical documentation updates

Answer: C,D,E,F (LEAVE A REPLY)

is incorrect. Residual risk is not an output of risk response. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk. As, Risk = Threat Vulnerabilityand Total risk = Threat Vulnerability Asset Value Residual risk can be calculated with the following formula: Residual Risk = Total Risk - Controls Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, transferred, mitigated or accepted. They also decide what controls to implement. Any loss due to their decisions falls on their sides. Residual risk assessments are conducted after mitigation to determine the impact of the risk on the enterprise. For risk assessment, the effect and frequency is reassessed and the impact is recalculated. Answer: A is incorrect. Risk priority number is not an output for risk response but instead it is done before applying response. Hence it act as one of the inputs of risk response and is not the output of it.

NEW QUESTION: 133

Which of the following BEST ensures that a firewall is configured in compliance with an enterprise's security policy?

A. Interview the firewall administrator.

B. Review the actual procedures.

C. Review the device's log file for recent attacks.

D. Review the parameter settings.

Answer: D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide reliable audit evidence documentation.

Incorrect Answers:

A: While interviewing the firewall administrator may provide a good process overview, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

B: While procedures may provide a good understanding of how the firewall is supposed to be managed, they do not reliably confirm that the firewall configuration complies with the enterprise's security policy.

C: While reviewing the device's log file for recent attacks may provide indirect evidence about the fact that logging is enabled, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

NEW QUESTION: 134

You are the project manager of GRT project. You discovered that by bringing on more qualified resources or by providing even better quality than originally planned, could result in reducing the

amount of time required to complete the project. If your organization seizes this opportunity it would be an example of what risk response?

A. Enhance

B. Exploit

C. Accept

D. Share

Answer: B (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project.

Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.

Incorrect Answers:

A: The enhance strategy closely watches the probability or impact of the risk event to assure that the organization realizes the benefits. The primary point of this strategy is to attempt to increase the probability and/or impact of positive C: Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs.

D: The share strategy is similar as transfer because in this a portion of the risk is shared with an external organization or another internal entity.

NEW QUESTION: 135

How residual risk can be determined?

A. By determining remaining vulnerabilities after countermeasures are in place.

B. By transferring all risks.

C. By threat analysis

D. By risk assessment

E. Explanation:

All risks are determined by risk assessment, regardless whether risks are residual or not.

F. is incorrect. Determining remaining vulnerabilities after countermeasures are in place says nothing about threats, therefore risk cannot be determined.

G. is incorrect. Risk cannot be determined by threat analysis alone, regardless whether it is residual or not.

Answer: D,E,F,G (LEAVE A REPLY)

is incorrect. Transferring all the risks in not relevant to determining residual risk. It is one of the method of risk management.

NEW QUESTION: 136

Whose risk tolerance matters MOST when making a risk decision?

A. The information security manager
B. Customers who would be affected by a breach
C. Auditors, regulators and standards organizations
D. The business process owner of the exposed assets
Answer: C (LEAVE A REPLY)

NEW QUESTION: 137
Which of the following is MOST important to include in regulatory and risk updates when a new legal requirement affects the organization?
A. Recommended key risk indicator (KRI) thresholds.
B. Cost of changes to critical business processes.
C. Risk associated with noncompliance.
D. Time frame to remediate noncompliance risk.
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 138
Which of the following is the PRIMARY reason to have the risk management process reviewed by a third party?
A. Obtain an objective view of process gaps and systemic errors.
B. Ensure the risk profile is defined and communicated.
C. Validate the threat management process.
D. Obtain objective assessment of the control environment.
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 139
Which of the following matrices is used to specify risk thresholds?
A. Risk indicator matrix
B. Impact matrix
C. Risk scenario matrix
D. Probability matrix

E. Explanation:
Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Answer: A (LEAVE A REPLY)
and B are incorrect. Estimation of risk's consequence and priority for awareness is conducted by using probability and impact matrix. These matrices specify the mixture of probability and impact that directs to rating the risks as low, moderate, or high priority. Answer: C is incorrect. A risk scenario is a description of an event that can lay an impact on business, when and if it would occur. Some examples of risk scenario are of: Having a major hardware failure Failed disaster recovery planning (DRP) Major software failure

NEW QUESTION: 140
A global organization is considering the acquisition of a competitor. Senior management has requested a review of the overall risk profile from the targeted organization.
Which of the following components of this review would provide the MOST useful information?
A. Risk appetite statement
B. Risk management policies
C. Risk register
D. Enterprise risk management framework
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 141
Which of the following should be an element of the risk appetite of an organization?
A. The residual risk affected by preventive controls
B. The effectiveness of compensating controls
C. The enterprise's capacity to absorb loss
D. The amount of inherent risk considered appropriate
Answer: C (LEAVE A REPLY)

NEW QUESTION: 142
You are the project manager of a SGT project. You have been actively communicating and working with the project stakeholders. One of the outputs of the "manage stakeholder expectations" process can actually create new risk events for your project. Which output of the manage stakeholder expectations process can create risks?
A. Project management plan updates
B. An organizational process asset updates
C. Change requests
D. Project document updates

E. Explanation:
The manage stakeholder expectations process can create change requests for the project, which can cause new risk events to enter into the project.
Change requests are requests to expand or reduce the project scope, modify policies, processes, plans, or procedures, modify costs or budgets or revise schedules. These requests for a change can be direct or indirect, externally or internally initiated, and legally or contractually imposed or optional. A Project Manager needs to ensure that only formally documented requested changes are processed and
only approved change requests are implemented.
F. is incorrect. The project management plan updates do not create new risks.
G. is incorrect. The project document updates do not create new risks.
Answer: C (LEAVE A REPLY)
is incorrect. The organizational process assets updates do not create new risks.

NEW QUESTION: 143
What are the requirements of effectively communicating risk analysis results to the relevant stakeholders?
Each correct answer represents a part of the solution. Choose three.
A. The results should be reported in terms and formats that are useful to support business decisions
B. Communicate only the negative risk impacts of events in order to drive response decisions
C. Communicate the risk-return context clearly
D. Provide decision makers with an understanding of worst-case and most probable scenarios
Answer: A,C,D (LEAVE A REPLY)
Section: Volume C
Explanation:
The result of risk analysis process is being communicated to relevant stakeholders. The steps that are involved in communication are:
* The results should be reported in terms and formats that are useful to support business decisions.
* Coordinate additional risk analysis activity as required by decision makers, like report rejection and scope adjustment.
* Communicate the risk-return context clearly, which include probabilities of loss and/or gain, ranges, and confidence levels (if possible) that enable management to balance risk-return.
* Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process.
* Provide decision makers with an understanding of worst-case and most probable scenarios, due diligence exposures and significant reputation, legal or regulatory considerations.
Incorrect Answers:

B: Both the negative and positive risk impacts are being communicated to relevant stakeholders. Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process.

NEW QUESTION: 144
Which of the following would be MOST beneficial as a key risk indicator (KRI)?
A. Negative security return on investment (ROI)
B. Project cost variances
C. Annualized loss projections
D. Current capital allocation reserves
Answer: (SHOW ANSWER)

NEW QUESTION: 145
From a risk management perspective, which of the following is the PRIMARY benefit of using automated system configuration validation tools?
A. Operational costs are reduced.
B. Staff costs are reduced.
C. Residual risk is reduced.
D. Inherent risk is reduced.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 146
An organization has introduced risk ownership to establish clear accountability for each process. To ensure effective risk ownership, it is MOST important that:
A. segregation of duties exists between risk and process owners.
B. risk owners have decision-making authority.
C. process ownership aligns with IT system ownership.
D. senior management has oversight of the process.
Answer: (SHOW ANSWER)

NEW QUESTION: 147
The risk associated with an asset before controls are applied can be expressed as:
A. the likelihood of a given threat.
B. the magnitude of an impact.
C. a function of the likelihood and impact.
D. a function of the cost and effectiveness of controls.
Answer: C (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 148
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of an anti-virus program?
A. Frequency of anti-virus software updates
B. Number of alerts generated by the anti-virus software
C. Number of false positives detected over a period of time
D. Percentage of IT assets with current malware definitions
Answer: D (LEAVE A REPLY)

NEW QUESTION: 149
Which of the following characteristics of risk controls can be defined as under?
"The separation of controls in the production environment rather than the separation in the design and implementation of the risk"
A. Trusted source
B. Secure
C. Distinct
D. Independent
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A control or countermeasure which does not overlap in its performance with another control or countermeasure is considered as distinct. Hence the separation of controls in the production environment rather than the separation in the design and implementation of the risk refers to distinct.
Incorrect Answers:
A: Trusted source refers to the commitment of the people designing, implementing, and maintenance of the control towards the security policy.
B: Secure controls refers to the activities ability to protect from exploitation or attack.
D: The separation in design, implementation, and maintenance of controls or countermeasures are refer to as independent. Hence this answer is not valid.

NEW QUESTION: 150
Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profit. If your organization seizes this opportunity it would be an example of what risk response?
A. Enhancing
B. Positive
C. Opportunistic
D. Exploiting
E. Explanation:

This is an example of exploiting a positive risk - a by-product of a project is an excellent example of exploiting a risk. Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.

Answer: (SHOW ANSWER)

is incorrect. Opportunistic is not a valid risk response. Answer: B is incorrect. This is an example of a positive risk, but positive is not a risk response. Answer: A is incorrect. Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.

NEW QUESTION: 151

Which of the following BEST enables the identification of trends in risk levels?

A. Qualitative definitions for key risk indicators (KRIs) are used.

B. Quantitative measurements are used for key risk indicators (KRIs).

C. Correlation between risk levels and key risk indicators (KRIs) is positive.

D. Measurements for key risk indicators (KRIs) are repeatable

Answer: A (LEAVE A REPLY)

NEW QUESTION: 152

Who is BEST suited to determine whether a new control properly mitigates data loss risk within a system?

A. Control owner

B. Risk owner

C. Data owner

D. System owner

Answer: D (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 153

Which of the following is an example of the second line in the three lines of defense model?

A. External auditors

B. Internal auditors
C. Risk management committee
D. Risk owners
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 154
Which of the following is a risk practitioner's BEST course of action upon learning that a control under internal review may no longer be necessary?
A. Update the status of the control as obsolete
B. Consult the internal auditor for a second opinion.
C. Obtain approval to retire the control.
D. Verify the effectiveness of the original mitigation plan.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 155
Which of the following is the BEST way to determine software license compliance?
A. Conduct periodic compliance reviews.
B. List non-compliant systems in the risk register.
C. Monitor user software download activity.
D. Review whistleblower reports of noncompliance.
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 156
Which of the following is MOST important to enable well-informed cybersecurity risk decisions?
A. Engage a third party to perform a risk assessment.
B. Determine and understand the risk rating of scenarios.
C. Identify roles and responsibilities for security controls.
D. Conduct risk assessment peer reviews.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 157
You are elected as the project manager of GHT project. You are in project initialization phase and are busy in defining requirements for your project. While defining requirements you are describing how users will interact with a system. Which of the following requirements are you defining here?
A. Technical requirement
B. Project requirement
C. Functional requirement
D. Business requirement
E. Explanation:

While defining requirements, there is need to define three requirements of the project- Business requirement, Functional requirement, and
Technical requirement
Functional requirements and use case models describe how users will interact with a system. Therefore here in this stem you are defining the functional requirement of the project.
F. is incorrect. Business requirements contain descriptions of what a system should do.
G. is incorrect. Technical requirements and design specifications and coding specifications describe how the system will interact, conditions under which the system will operate and the information criteria the system should meet.
Answer: C (LEAVE A REPLY)
is incorrect. Business requirement, Functional requirement, and Technical requirement come under project requirement. In this stem it is particular defining the functional requirement, hence this is not the best answer.

NEW QUESTION: 158
Which of the following data would be used when performing a business impact analysis (BIA)?
A. Cost of regulatory compliance
B. Expected costs for recovering the business
C. Cost-benefit analysis of running the current business
D. Projected impact of current business on future business
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 159
Reviewing results from which of the following is the BEST way to identify information systems control deficiencies?
A. Control self-assessment (CSA)
B. Vulnerability and threat analysis
C. User acceptance testing (UAT)
D. Control remediation planning
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 160
Which of the following BEST represents a critical threshold value for a key control indicator (KCI)?
A. A value that represents the intended control state
B. Thresholds benchmarked to peer organizations
C. A typical operational value
D. The value at which control effectiveness would fail
Answer: (SHOW ANSWER)

NEW QUESTION: 161
The BEST way to justify the risk mitigation actions recommended in a risk assessment would be to:
A. focus on the business drivers
B. reference best practice
C. benchmark with competitor's actions
D. align with audit results
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 162
Which of the following events refer to loss of integrity?
Each correct answer represents a complete solution. Choose three.
A. Someone sees company's secret formula
B. Someone makes unauthorized changes to a Web site
C. An e-mail message is modified in transit
D. A virus infects a file
Answer: B,C,D (LEAVE A REPLY)
Section: Volume C
Explanation/Reference:
Explanation:
Loss of integrity refers to the following types of losses:
* An e-mail message is modified in transit A virus infects a file
* Someone makes unauthorized changes to a Web site
Incorrect Answers:
A: Someone sees company's secret formula or password comes under loss of confidentiality.

NEW QUESTION: 163
Which of the following should be the MOST important consideration when determining controls necessary for a highly critical information system?
A. The number of vulnerabilities to the system
B. The level of acceptable risk to the organization
C. The organization's available budget
D. The number of threats to the system
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 164

You work as a project manager for BlueWell Inc. You have declined a proposed change request because of the risk associated with the proposed change request. Where should the declined change request be documented and stored?

A. Change request log

B. Project archives

C. Lessons learned

D. Project document updates

Answer: (SHOW ANSWER)

Section: Volume B

Explanation:

The change request log records the status of all change requests, approved or declined.

The change request log is used as an account for change requests and as a means of tracking their disposition on a current basis. The change request log develops a measure of consistency into the change management process. It encourages common inputs into the process and is a common estimation approach for all change requests. As the log is an important component of project requirements, it should be readily available to the project team members responsible for project delivery. It should be maintained in a file with read-only access to those who are not responsible for approving or disapproving project change requests.

Incorrect Answers:

B: The project archive includes all project documentation and is created through the close project or phase process. It is not the best choice for this option.

C: Lessons learned are not the correct place to document the status of a declined, or approved, change request.

D: The project document updates is not the best choice for this question. It can be placed into the project documents, but the declined changes are part of the change request log.

NEW QUESTION: 165

You are the project manager of project for a client. The client has promised your company a bonus, if the project is completed early. After studying the project work, you elect to crash the project in order to realize the early end date. This is an example of what type of risk response?

A. Negative risk response, because crashing will add risks.

B. Positive risk response, as crashing is an example of enhancing.

C. Positive risk response, as crashing is an example of exploiting.

D. Negative risk response, because crashing will add costs.

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

This is a positive risk response, as crashing is an example of enhancing. You are enhancing the probability of finishing the project early to realize the reward of bonus. Enhancing doesn't ensure positive risks, but it does increase the likelihood of the event.

Incorrect Answers:

A: Crashing is a positive risk response. Generally, crashing doesn't add risks and is often confused with other predominant schedule compression techniques of fast tracking - which does add risks.
C: This isn't an example of exploiting. Exploiting is an action to take advantage of a positive risk response that will happen.
D: Crashing does add costs, but in this instance, crashing is an example of the positive risk response of enhancing.

NEW QUESTION: 166
What are the three PRIMARY steps to be taken to initialize the project?
Each correct answer represents a complete solution. Choose all that apply.
A. Conduct a feasibility study
B. Define requirements
C. Acquire software
D. Plan risk management
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Projects are initiated by sponsors who gather the information required to gain approval for the project to be created. Information often compiled into the terms of a project charter includes the objective of the project, business case and problem statement, stakeholders in the system to be produced, and project manager and sponsor.
Following are the steps to initiate the project:
Conduct a feasibility study: Feasibility study starts once initial approval has been given to move forward
with a project, and includes an analysis to clearly define the need and to identify alternatives for addressing the need. A feasibility study involves:
- Analyzing the benefits and solutions for the identified problem area
- Development of a business case that states the strategic benefits of implementing the system either in productivity gains or in future cost avoidance and identifies and quantifies the cost savings of the new system.
- Estimation of a payback schedule for the cost incurred in implementing the system or shows the projected return on investment (ROI) Define requirements: Requirements include:
- Business requirements containing descriptions of what a system should do
- Functional requirements and use case models describing how users will interact with a system
- Technical requirements and design specifications and coding specifications describing how the system will interact, conditions under which the system will operate and the information criteria the system should meet.
Acquire software: Acquiring software involves building new or modifying existing hardware or software

after final approval by the stakeholder, which is not a phase in the standard SDLC process. If a decision was reached to acquire rather than develop software, this task should occur after defining requirements.
Incorrect Answers:
D: Risk management is planned latter in project development process, and not during initialization.

NEW QUESTION: 167
Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?
A. Service level agreement (SLA)
B. Independent audit report
C. Business impact analysis (BIA)
D. Nondisclosure agreement (NDA)
Answer: (SHOW ANSWER)

NEW QUESTION: 168
Which of the following role carriers will decide the Key Risk Indicator of the enterprise?
Each correct answer represents a part of the solution. Choose two.
A. Business leaders
B. Senior management
C. Human resource
D. Chief financial officer
E. Explanation:
An enterprise may have hundreds of risk indicators such as logs, alarms and reports. The CRISC will usually need to work with senior management and business leaders to determine which risk indicators will be monitored on a regular basis and be recognized as KRIs.
Answer: A,B (LEAVE A REPLY)
and C are incorrect. Chief financial officer and human resource only overview common risk view, but are not involved in risk based decisions.

NEW QUESTION: 169

The MAIN purpose of conducting a control self-assessment (CSA) is to:
A. gain a better understanding of the risk in the organization
B. reduce the dependency on external audits
C. gain a better understanding of the control effectiveness in the organization
D. adjust the controls prior to an external audit
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?
A. Modify the action plan in the risk register.
B. Seek approval from the previous action plan manager.
C. Communicate the decision to the risk owner for approval
D. Identify an owner for the new control.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
Which of the following baselines identifies the specifications required by the resource that meet the approved requirements?
A. Functional baseline
B. Allocated baseline
C. Product baseline
D. Developmental baseline
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Allocated baseline identifies the specifications that meet the approved requirements.
Incorrect Answers:
A: Functional baseline identifies the initial specifications before any changes are made.
C: Product baseline identifies the minimal specification required by the resource to meet business outcomes.
D: Developmental baseline identifies the state of the resources as it is developed to meet or exceed expectations and requirements.

NEW QUESTION: 172
Which of the following is the BEST control to detect an advanced persistent threat (APT)?
A. Monitoring social media activities
B. Conducting regular penetration tests
C. Utilizing antivirus systems and firewalls
D. Implementing automated log monitoring

Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 173
Which of the following assets are the examples of intangible assets of an enterprise?
Each correct answer represents a complete solution. Choose two.
A. Customer trust
B. Information
C. People
D. Infrastructure
Answer: A,B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Assets are the economic resources owned by business or company. Anything tangible or intangible that one possesses, usually considered as applicable to the payment of one's debts, is considered an asset. An asset can also be defined as a resource, process, product, computing infrastructure, and so forth that an organization has determined must be protected.
Tangible asset: Tangible are those assets that has physical attributes and can be detected with the senses, e.g., people, infrastructure, and finances.
Intangible asset: Intangible are those assets that has no physical attributes and cannot be detected with the senses, e.g., information, reputation and customer trust.

NEW QUESTION: 174
Which of the following is an output of risk assessment process?
A. Identification of risk
B. Identification of appropriate controls
C. Mitigated risk
D. Enterprise left with residual risk
E. Explanation:
The output of the risk assessment process is identification of appropriate controls for reducing or eliminating risk during the risk mitigation process. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT system.
Once risk factors have been identified, existing or new controls are designed and measured for their strength and likelihood of effectiveness. Controls are preventive, detective or corrective; manual or programmed; and formal or ad hoc.
F. is incorrect. Risk identification acts as input of the risk assessment process.
G. is incorrect. Residual risk is the latter output after appropriate control.
Answer: (SHOW ANSWER)
is incorrect. This is an output of risk mitigation process,that is, after applying several risk responses.

NEW QUESTION: 175
Which of the following will significantly affect the standard information security governance model?
A. Currency with changing legislative requirements
B. Number of employees
C. Complexity of the organizational structure
D. Cultural differences between physical locations
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Complexity of the organizational structure will have the most significant impact on the Information security governance model. Some of the elements that impact organizational structure are multiple business units and functions across the organization.
Incorrect Answers:
A: Currency with changing legislative requirements should not have major impact once good governance models are placed, hence, governance will help in effective management of the organization's ongoing compliance.
B, D: The numbers of employees and the distance between physical locations have less impact on Information security models as well-defined process, technology and people components together provide the proper governance.

NEW QUESTION: 176
it was determined that replication of a critical database used by two business units failed. Which of the following should be of GREATEST concern1?
A. The cost of recovering the data
B. The underutilization of the replicated link
C. The lack of integrity of data
D. The loss of data confidentiality
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
Which of the following is the MOST important consideration when selecting key risk indicators (KRIs) to monitor risk trends over time?
A. Availability of automated reporting systems
B. Ability to aggregate data
C. Ability to predict trends
D. Ongoing availability of data
Answer: A (LEAVE A REPLY)

NEW QUESTION: 178

Which of the following BEST indicates whether security awareness training is effective?
A. User self-assessment
B. Course evaluation
C. User behavior after training
D. Quality of training materials
Answer: (SHOW ANSWER)

NEW QUESTION: 179
A risk owner should be the person accountable for:
A. the risk management process
B. managing controls.
C. the business process.
D. implementing actions.
Answer: (SHOW ANSWER)

NEW QUESTION: 180
In an organization with a mature risk management program, which of the following would provide the BEST evidence that the IT risk profile is up to date?
A. Risk questionnaire
B. Risk register
C. Compliance manual
D. Management assertion
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 181
What are the requirements of effectively communicating risk analysis results to the relevant stakeholders? Each correct answer represents a part of the solution. Choose three.
A. The results should be reported in terms and formats that are useful to support business decisions
B. Communicate only the negative risk impacts of events in order to drive response decisions
C. Communicate the risk-return context clearly
D. Provide decision makers with an understanding of worst-case and most probable scenarios
E. Explanation:
The result of risk analysis process is being communicated to relevant stakeholders. The steps that are involved in communication are: The results should be reported in terms and formats that are useful to support business decisions. Coordinate additional risk analysis activity as required by decision makers, like report rejection and scope adjustment. Communicate the risk-return context clearly, which include probabilities of loss and/or gain, ranges, and confidence levels (if possible) that enable management to balance risk-return. Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities

which should channel back into the strategy and objective setting process. Provide decision makerswith an understanding of worst-case and most probable scenarios, due diligence exposures and significant reputation, legal or regulatory considerations.

Answer: (SHOW ANSWER)

is incorrect. Both the negative and positive risk impacts are being communicated to relevant stakeholders. Identify the negative impacts of events that drive response decisions as well as positive impacts of events that represent opportunities which should channel back into the strategy and objective setting process.

NEW QUESTION: 182

Ned is the project manager of the HNN project for your company. Ned has asked you to help him complete some probability distributions for his project. What portion of the project will you most likely use for probability distributions?

A. Bias towards risk in new resources

B. Risk probability and impact matrixes

C. Uncertainty in values such as duration of schedule activities

D. Risk identification

E. Explanation:

Risk probability distributions are likely to be utilized in uncertain values, such as time and cost estimates for a project.

F. is incorrect. Risk probability distributions are not likely the risk identification.

G. is incorrect. Risk probability distributions are not likely to be used with risk probability and impact matrices.

Answer: (SHOW ANSWER)

is incorrect. Risk probability distributions do not typically interact with the bias towards risks in new resources.

NEW QUESTION: 183

Which of the following provides the MOST useful information to determine risk exposure following control implementations?

A. Policies, standards, and procedures

B. Risk limits, thresholds, and indicators

C. Strategic plan and risk management integration
D. Risk escalation and process for communication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 184
Which of the following is MOST important for maintaining the effectiveness of an IT risk register?
A. Recording and tracking the status of risk response plans within the register.
B. Communicating the register to key stakeholders.
C. Performing regular reviews and updates to the register.
D. Removing entries from the register after the risk has been treated.
Answer: (SHOW ANSWER)
Section: Volume D
Explanation

NEW QUESTION: 185
The MAIN goal of the risk analysis process is to determine the:
A. frequency and magnitude of loss
B. potential severity of impact
C. threats and vulnerabilities
D. control deficiencies
Answer: A (LEAVE A REPLY)

NEW QUESTION: 186
Which of the following is NOT true for Key Risk Indicators?
A. They are selected as the prime monitoring indicators for the enterprise
B. They help avoid having to manage and report on an excessively large number of risk indicators
C. The complete set of KRIs should also balance indicators for risk, root causes and business impact.
D. They are monitored annually
E. Explanation:
They are monitored on regular basis as they indicate high probability and high impact risks. As risks change over time, hence KRIs should also be monitored regularly for its effectiveness on these changing risks.
Answer: D,E (LEAVE A REPLY)
B, and C are incorrect. These all are true for KRIs. Key Risk Indicators are the prime monitoring indicators of the enterprise. KRIs are highly relevant and possess a high probability of predicting or indicating important risk. KRIs help in avoiding excessively large number of risk indicators to manage and report that a large enterprise may have. The complete set of KRIs should also balance indicators for risk, root causes and business impact, so as to indicate the risk and its impact completely.

NEW QUESTION: 187
During an IT department reorganization, the manager of a risk mitigation action plan was replaced. The new manager has begun implementing a new control after identifying a more effective option. Which of the following is the risk practitioner's BEST course of action?
A. Communicate the decision to the risk owner for approval
B. Identify an owner for the new control
C. Modify the action plan in the risk register
D. Seek approval from the previous action plan manager
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 188
A control for mitigating risk in a key business area cannot be implemented immediately. Which of the following is the risk practitioner's BEST course of action when a compensating control needs to be applied?
A. Record the risk as accepted m the risk register.
B. update the risk response plan.
C. Obtain the risk owner's approval.
D. Inform senior management.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 189
The acceptance of control costs that exceed risk exposure is MOST likely an example of:
A. corporate culture misalignment.
B. corporate culture alignment.
C. high risk tolerance
D. low risk tolerance.
Answer: (SHOW ANSWER)

NEW QUESTION: 190
Which of the following is PRIMARILY a risk management responsibly of the first line of defense?
A. Validating the status of risk mitigation efforts
B. Conducting independent reviews of risk assessment results
C. Establishing risk policies and standards
D. Implementing risk treatment plans
Answer: C (LEAVE A REPLY)

NEW QUESTION: 191
Which of the following is the MOST important consideration when identifying stakeholders to review risk scenarios developed by a risk analyst? The reviewers are:
A. accountable for the affected processes.

B. independent from the business operations.
C. members of senior management.
D. authorized to select risk mitigation options.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 192
An application owner has specified the acceptable downtime in the event of an incident to be much lower than the actual time required for the response team to recover the application. Which of the following should be the NEXT course of action?
A. Prepare a cost-benefit analysis of alternatives available
B. Invoke the disaster recovery plan during an incident.
C. Implement redundant infrastructure for the application.
D. Reduce the recovery time by strengthening the response team.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 193
Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profit. If your organization seizes this opportunity, it would be an example of what risk response?
A. Enhancing
B. Positive
C. Opportunistic
D. Exploiting
Answer: D (LEAVE A REPLY)
Section: Volume C
Explanation:
This is an example of exploiting a positive risk - a by-product of a project is an excellent example of exploiting a risk. Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.
Incorrect Answers:
A: Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.
B: This is an example of a positive risk, but positive is not a risk response.
C: Opportunistic is not a valid risk response.

NEW QUESTION: 194
Which of the following is a risk practitioner's BEST recommendation to address an organization's need to secure multiple systems with limited IT resources?

A. Apply available security patches.
B. Perform a vulnerability analysis.
C. Conduct a business impact analysis (BIA)
D. Schedule a penetration test.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 195
A change management process has recently been updated with new testing procedures. What is the NEXT course of action?
A. Conduct a cost-benefit analysis to justify the cost of the control
B. Assess the maturity of the change management process.
C. Communicate to those who test and promote changes.
D. Monitor processes to ensure recent updates are being followed.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 196
Which of the following BEST describes the utility of a risk?
A. The finance incentive behind the risk
B. The potential opportunity of the risk
C. The mechanics of how a risk works
D. The usefulness of the risk to individuals or groups
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The utility of the risk describes the usefulness of a particular risk to an individual. Moreover, the same risk can be utilized by two individuals in different ways. Financial outcomes are one of the methods for measuring potential value for taking a risk. For example, if the individual's economic wealth increases, the potential utility of the risk will decrease.
Incorrect Answers:
A: Determining financial incentive is one of the method to measure the potential value for taking a risk, but it is not the valid definition for utility of risk.
B: It is not the valid definition.
C: It is not the valid definition.

NEW QUESTION: 197
A risk practitioner discovers several key documents detailing the design of a product currently in development have been posted on the Internet. What should be the risk practitioner's FIRST course of action?
A. Conduct an immediate risk assessment
B. Inform internal audit.
C. invoke the established incident response plan.
D. Perform a root cause analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 198
Which of the following is the MOST important component in a risk treatment plan?
A. Target completion date
B. Treatment plan ownership
C. Treatment plan justification
D. Technical details
Answer: C (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 199
The FIRST task when developing a business continuity plan should be to:
A. identify critical business functions and resources.
B. determine data backup and recovery availability at an alternate site.
C. define roles and responsibilities for implementation.
D. identify recovery time objectives (RTOs) for critical business applications.
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 200
An assessment of information security controls has identified ineffective controls. Which of the following should be the risk practitioner's FIRST course of action?
A. Deploy a compensating control to address the identified deficiencies
B. Report the ineffective control for inclusion in the next audit report
C. Determine if the impact is outside the risk appetite
D. Request a formal acceptance of risk from senior management
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 201
You work as a project manager for BlueWell Inc. Your project is using a new material to construct a large warehouse in your city. This new material is cheaper than traditional building materials, but it takes some time to learn how to use the material properly. You have communicated to the project stakeholders that you will be able to save costs by using the new material, but you will need a few extra weeks to complete training to use the materials. This risk response of learning how to use the new materials can also be known as what term?
A. Benchmarking
B. Cost-benefits analysis
C. Cost of conformance to quality
D. Team development
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
When the project team needs training to be able to complete the project work it is a cost of conformance to quality.
The cost of conformance to quality defines the cost of training, proper resources, and the costs the project must spend in order to ascertain the expected levels of quality the customer expects from the project. It is the capital used up throughout the project to avoid failures. It consists of two types of costs:
Prevention costs: It is measured to build a quality product. It includes costs in training, document
- processing, equipment, and time to do it right.
Appraisal costs: It is measured to assess the quality. It includes testing, destructive testing loss, and
- inspections.
Incorrect Answers:
A: Benchmarking compares any two items, such as materials, vendors, or resources.
B: Cost-benefit analysis is the study of the benefits in relation to the costs to receive the benefits of a decision, a project, or other investment.
D: Team development describes activities the project manager uses to create a more cohesive and responsive project team.

NEW QUESTION: 202
The PRIMARY benefit associated with key risk indicators (KRIs) is that they:
A. identify trends in the organization's vulnerabilities
B. provide ongoing monitoring of emerging risk
C. help an organization identify emerging threats
D. benchmark the organization's risk profile
Answer: C (LEAVE A REPLY)

Section: Volume D
Explanation/Reference: https://www.isaca.org/COBIT/Documents/Risk-IT-Framework_fmk_Eng_0610.pdf

NEW QUESTION: 203
Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?
A. Creating modules for targeted audiences
B. Piloting courses with focus groups
C. Using reputable third-party training programs
D. Reviewing content with senior management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 204
Which of the following provides the MOST helpful reference point when communicating the results of a risk assessment to stakeholders?
A. Risk awareness
B. Risk policy
C. Risk appetite
D. Risk tolerance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 205
Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?
A. Business Continuity Strategy
B. Index of Disaster-Relevant Information
C. Disaster Invocation Guideline
D. Availability/ ITSCM/ Security Testing Schedule
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Business Continuity Strategy is an outline of the approach to ensure the continuity of Vital Business Functions in the case of disaster events. The Business Continuity Strategy is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy.
Incorrect Answers:
B: Index of Disaster-Relevant Information is a catalog of all information that is relevant in the event of disasters. This document is maintained and circulated by IT Service Continuity Management to all members of IT staff with responsibilities for fighting disasters.
C: Disaster Invocation Guideline is a document produced by IT Service Continuity Management with detailed instructions on when and how to invoke the procedure for fighting a disaster. Most

importantly, the guideline defines the first step to be taken by the Service Desk after learning that a disaster has occurred.
D: Availability/ ITSCM/ Security Testing Schedule is a schedule for the regular testing of all availability, continuity, and security mechanisms jointly maintained by Availability, IT Service Continuity, and IT Security Management.

NEW QUESTION: 206
You are the risk official in Bluewell Inc. You are supposed to prioritize several risks. A risk has a rating for occurrence, severity, and detection as 4, 5, and 6, respectively. What Risk Priority Number (RPN) you would give to it?
A. 120
B. 100
C. 15
D. 30
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Steps involving in calculating risk priority number are as follows:
Identify potential failure effects
- Identify potential causes
- Establish links between each identified potential cause
- Identify potential failure modes
- Assess severity, occurrence and detection
- Perform score assessments by using a scale of 1 -10 (low to high rating) to score these assessments.
- Compute the RPN for a particular failure mode as Severity multiplied by occurrence and detection.
- RPN = Severity * Occurrence * Detection

Hence,
RPN = 4 * 5 * 6
= 120
Incorrect Answers:
B, C, D: These are not RPN for given values of severity, occurrence, and detection.

NEW QUESTION: 207
Which of the following BEST indicates the effectiveness of anti-malware software?
A. Number of patches made to anti-malware software
B. Number of downtime hours in business critical servers
C. Number of successful attacks by malicious software

D. Number of staff hours lost due to malware attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 208
Your project is an agricultural-based project that deals with plant irrigation systems. You have discovered a byproduct in your project that your organization could use to make a profit. If your organization seizes this opportunity it would be an example of what risk response?
A. Enhancing
B. Positive
C. Opportunistic
D. Exploiting
Answer: D (LEAVE A REPLY)
Section: Volume A
Explanation
Explanation:
This is an example of exploiting a positive risk - a by-product of a project is an excellent example of exploiting a risk. Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.
Incorrect Answers:
A: Enhancing is a positive risk response that describes actions taken to increase the odds of a risk event to happen.
B: This is an example of a positive risk, but positive is not a risk response.
C: Opportunistic is not a valid risk response.

NEW QUESTION: 209
Which of the following are true for threats?
Each correct answer represents a complete solution. Choose three.
A. They can become more imminent as time goes by, or it can diminish
B. They can result in risks from external sources
C. They are possibility
D. They are real
E. They will arise and stay in place until they are properly dealt.
Answer: A,B,D (LEAVE A REPLY)
Section: Volume C
Explanation:
Threat is an act of coercion wherein an act is proposed to elicit a negative response. Threats are real, while the vulnerabilities are a possibility. They can result in risks from external sources, and can become imminent by time or can diminish.

Incorrect Answers:
C, E: These two are true for vulnerability, but not threat. Unlike the threat, vulnerabilities are possibility and can result in risks from internal sources. They will arise and stay in place until they are properly dealt.

NEW QUESTION: 210
Which of the following is a technique that provides a systematic description of the combination of unwanted occurrences in a system?
A. Sensitivity analysis
B. Scenario analysis
C. Fault tree analysis
D. Cause and effect analysis
Answer: C (LEAVE A REPLY)
Section: Volume A
Explanation:
Fault tree analysis (FIA) is a technique that provides a systematic description of the combination of possible occurrences in a system, which can result in an undesirable outcome. It combines hardware failures and human failures.
Incorrect Answers:
A: Sensitivity analysis is the quantitative risk analysis technique that:
Assist in determination of risk factors that have the most potential impact Examines the extent to which the uncertainty of each element affects the object under consideration when all other uncertain elements are held at their baseline values B: This analysis provides ability to see a range of values across several scenarios to identify risk in specific situation. It provides ability to identify those inputs which will provide the greatest level of uncertainty.
D: Cause-and-effect analysis involves the use of predictive or diagnostic analytical tool for exploring the root causes or factors that contribute to positive or negative effects or outcomes. These tools also help in identifying potential risk.

NEW QUESTION: 211
Which of the following BEST enables a risk practitioner to enhance understanding of risk among stakeholders?
A. Threat analysis
B. Key risk indicators
C. Risk scenarios
D. Business impact analysis
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 212
Which of the following phases is involved in the Data Extraction, Validation, Aggregation and Analysis?
A. Risk response and Risk monitoring
B. Requirements gathering, Data access, Data validation, Data analysis, and Reporting and corrective action
C. Data access and Data validation
D. Risk identification, Risk assessment, Risk response and Risk monitoring
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The basic concepts related to data extraction, validation, aggregation and analysis is important as KRIs often rely on digital information from diverse sources. The phases which are involved in this are:
Requirements gathering: Detailed plan and project's scope is required for monitoring risks. In the case
- of a monitoring project, this step should involve process owners, data owners, system custodians and other process stakeholders.
Data access: In the data access process, management identifies which data are available and how
- they can be acquired in a format that can be used for analysis. There are two options for data extraction:
- Extracting data directly from the source systems after system owner approval
- Receiving data extracts from the system custodian (IT) after system owner approval Direct extraction is preferred, especially since this involves management monitoring its own controls, instead of auditors/third parties monitoring management's controls. If it is not feasible to get direct access, a data access request form should be submitted to the data owners that detail the appropriate data fields to be extracted. The request should specify the method of delivery for the file.
Data validation: Data validation ensures that extracted data are ready for analysis. One of its important
-

objective is to perform tests examining the data quality to ensure data are valid complete and free of errors. This may also involve making data from different sources suitable for comparative analysis.
Following concepts should be considered while validating data:
- Ensure the validity, i.e., data match definitions in the table layout
- Ensure that the data are complete
- Ensure that extracted data contain only the data requested
- Identify missing data, such as gaps in sequence or blank records
- Identify and confirm the validity of duplicates
- Identify the derived values
- Check if the data given is reasonable or not
- Identify the relationship between table fields
- Record, in a transaction or detail table, that the record has no match in a master table Data analysis: Analysis of data involves simple set of steps or complex combination of commands and other functionality. Data analysis is designed in such a way to achieve the stated objectives from the project plan. Although this may be applicable to any monitoring activity, it would be beneficial to consider transferability and scalability. This may include robust documentation, use of software development standards and naming conventions.
Reporting and corrective action: According to the requirements of the monitoring objectives and the technology being used, reporting structure and distribution are decided. Reporting procedures indicate to whom outputs from the automated monitoring process are distributed so that they are directed to the right people, in the right format, etc. Similar to the data analysis stage, reporting may also identify areas in which changes to the sensitivity of the reporting parameters or the timing and frequency of the monitoring activity may be required.
Incorrect Answers:
D: These are the phases that are involved in risk management.

NEW QUESTION: 213
What is the PRIMARY reason to periodically review key performance indicators (KPIs)?
A. Identify trends
B. Optimize resources needed for controls
C. Ensure compliance
D. Promote a risk-aware culture
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 214
The BEST way to determine the likelihood of a system availability risk scenario is by assessing the:

A. availability of fault tolerant software
B. strategic plan for business growth
C. vulnerability scan results of critical systems
D. redundancy of technical infrastructure
Answer: D (LEAVE A REPLY)

NEW QUESTION: 215
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
After a high-profile systems breach at an organization s key vendor, the vendor has implemented additional mitigating controls. The vendor has voluntarily shared the following set of assessments:
Which of the assessments provides the MOST reliable input to evaluate residual risk in the vendor's control environment?

Type	Scope	Completed By
External audit	Financial systems and processes	Third party
Internal audit	IT security risk management	Vendor
Vendor performance scorecard	Service level agreement compliance	Organization
Regulatory examination	Information security management program	Regulator

A. External audit
B. Vendor performance scorecard
C. Internal audit
D. Regulatory examination
Answer: C (LEAVE A REPLY)

NEW QUESTION: 216
Which of the following is of GREATEST concern when uncontrolled changes are made to the control environment?
A. An increase in the level of residual risk
B. A decrease in control layering effectiveness
C. An increase in inherent risk
D. An increase in control vulnerabilities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 217
A large organization is replacing its enterprise resource planning (ERP) system and has decided not to deploy the payroll module of the new system. Instead, the current payroll system will continue to be used. Of the following, who should own the risk if the ERP and payroll system fail to operate as expected?

A. The project steering committee
B. The business owner
C. The IT project manager
D. The ERP administrator
Answer: B (LEAVE A REPLY)

NEW QUESTION: 218
Which of the following is the PRIMARY requirement before choosing Key performance indicators of an enterprise?
A. Determine size and complexity of the enterprise
B. Prioritize various enterprise processes
C. Determine type of market in which the enterprise operates
D. Enterprise must establish its strategic and operational goals
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Key Performance Indicators is a set of measures that a company or industry uses to measure and/or compare performance in terms of meeting their strategic and operational goals. KPIs vary with company to company, depending on their priorities or performance criteria.
A company must establish its strategic and operational goals and then choose their KPIs which can best reflect those goals. For example, if a software company's goal is to have the fastest growth in its industry, its main performance indicator may be the measure of its annual revenue growth.
Incorrect Answers:
A: Determination of size and complexity of the enterprise is the selection criteria of the KRI, not KPI. KPI does not have any relevancy with size and complexity of the enterprise.
B: This is not the valid answer.
C: Type of market in which the enterprise is operating do not affect the selection of KPIs.

NEW QUESTION: 219
Which of the following processes addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget?
A. Monitor and Control Risk
B. Plan risk response
C. Identify Risks
D. Qualitative Risk Analysis
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The plan risk response project management process aims to reduce the threats to the project objectives and to increase opportunities. It follows the perform qualitative risk analysis process

and perform quantitative risk analysis process. Plan risk response process includes the risk response owner to take the job for each agreed-to and funded risk response. This process addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget.
The inputs to the plan risk response process are as follows:
Risk register
- Risk management plan
-
Incorrect Answers:
A: Monitor and Control Risk is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project. It can involve choosing alternative strategies, executing a contingency or fallback plan, taking corrective action, and modifying the project management plan.
C: Identify Risks is the process of determining which risks may affect the project. It also documents risks' characteristics. The Identify Risks process is part of the Project Risk Management knowledge area. As new risks may evolve or become known as the project progresses through its life cycle, Identify Risks is an iterative process. The process should involve the project team so that they can develop and maintain a sense of ownership and responsibility for the risks and associated risk response actions. Risk Register is the only output of this process.
D: Qualitative analysis is the definition of risk factors in terms of high/medium/low or a numeric scale (1 to
10). Hence it determines the nature of risk on a relative scale.
Some of the qualitative methods of risk analysis are:
Scenario analysis- This is a forward-looking process that can reflect risk for a given point in time.
- Risk Control Self -assessment (RCSA) - RCSA is used by enterprises (like banks) for the identification
-
and evaluation of operational risk exposure. It is a logical first step and assumes that business owners and managers are closest to the issues and have the most expertise as to the source of the risk. RCSA is a constructive process in compelling business owners to contemplate, and then explain, the issues at hand with the added benefit of increasing their accountability.

NEW QUESTION: 220
Which of the following documents is described in the statement below?
"It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."
A. Quality management plan
B. Risk management plan
C. Risk register
D. Project charter
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning.
Risk register is developed along with all processes of the risk management from Plan Risk Management through Monitor and Control Risks.
Incorrect Answers:
A: The quality management plan is a component of the project management plan. It describes how the project team will implement the organization's quality policy. The quality management plan addresses quality control (QC), quality assurance (QA), and continuous process improvement for the project. Based on the requirement of the project, the quality management plan may be formal or informal, highly detailed or broadly framed.
B: Risk management plan includes roles and responsibilities, risk analysis definitions, timing for reviews, and risk threshold. The Plan Risk Responses process takes input from risk management plan and risk register to define the risk response.
D: The project charter is the document that formally authorizes a project. The project charter provides the project manager with the authority to apply organizational resources to project activities.

NEW QUESTION: 221
Which of these documents is MOST important to request from a cloud service provider during a vendor risk assessment?
A. Nondisclosure agreement (NDA)
B. Service level agreement (SLA)
C. Independent audit report
D. Business impact analysis (BIA)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a disaster recovery plan (DRP)?
A. Number of users that participated in the DRP testing
B. Percentage of applications that met the RTO during DRP testing
C. Percentage of issues resolved as a result of DRP testing
D. Number of issues identified during DRP testing
Answer: (SHOW ANSWER)

NEW QUESTION: 223
Which of the following is the MOST effective key performance indicator (KPI) for change management?
A. Average time required to implement a change
B. Percentage of changes with a fallback plan

C. Number of changes implemented
D. Percentage of successful changes
Answer: (SHOW ANSWER)

NEW QUESTION: 224
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?
A. Control environment
B. KRI thresholds
C. Stakeholder requirements
D. Integrity of the source data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 225
When developing IT risk scenarios, it is CRITICAL to involve:
A. senior management
B. process owners
C. internal auditors
D. IT managers
Answer: (SHOW ANSWER)

NEW QUESTION: 226
An organization has raised the risk appetite for technology risk. The MOST likely result would be:
A. lower risk management cost
B. decreased residual risk
C. higher risk management cost
D. increased inherent risk
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 227
Which among the following is the MOST crucial part of risk management process?

A. Risk communication
B. Auditing
C. Risk monitoring
D. Risk mitigation
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risk communication is a critical part in the risk management process. People are naturally uncomfortable talking about risk and tend to put off admitting that risk is involved and communicating about issues; incidents; and; eventually, even crises.
If risk is to be managed and mitigated, it must first be discussed and effectively communicated throughout an enterprise.
Incorrect Answers:
B: Auditing is done to test the overall risk management process and the planned risk responses. So it is the very last phase after completion of risk management process.
C: Risk monitoring is the last phase to complete risk management process, and for proper management of risk it should be communicated properly. Hence risk communication is the most crucial step.
D: Risk mitigation is one of the phases of risk management process for effective mitigation of risk it should be first communicated throughout an enterprise.

NEW QUESTION: 228
An organization control environment is MOST effective when:
A. control designs are reviewed periodically
B. controls perform as intended.
C. controls are implemented consistently.
D. controls operate efficiently
Answer: (SHOW ANSWER)

NEW QUESTION: 229
A key risk indicator (KRI) is reported to senior management on a periodic basis as exceeding thresholds, but each time senior management has decided to take no action to reduce the risk. Which of the following is the MOST likely reason for senior management's response?
A. The underlying data source for the KRI is using inaccurate data and needs to be corrected.
B. The KRI threshold needs to be revised to better align with the organization's risk appetite.
C. Senior management does not understand the KRI and should undergo risk training.
D. The KRI is not providing useful information and should be removed from the KRI inventory.
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 230
An organization is considering the adoption of an aggressive business strategy to achieve desired growth From a risk management perspective what should the risk practitioner do NEXT?
A. Increase the scale for measuring impact due to threat materialization
B. Identify new threats resorting from the new business strategy
C. Update risk awareness training to reflect current levels of risk appetite and tolerance
D. Inform the board of potential risk scenarios associated with aggressive business strategies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 231
Which of the following operational risks ensures that the provision of a quality product is not overshadowed by the production costs of that product?
A. Information security risks
B. Contract and product liability risks
C. Project activity risks
D. Profitability operational risks
Answer: (SHOW ANSWER)
Section: Volume B
Explanation:
Profitability operational risks focus on the financial risks which encompass providing a quality product that is cost-effective in production. It ensures that the provision of a quality product is not overshadowed by the production costs of that product.
Incorrect Answers:
A: Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Information security risks are the risks that are associated with the protection of these information and information systems.
B: These risks do not ensure that the provision of a quality product is not overshadowed by the production costs of that product.
C: Project activity risks are not associated with provision of a quality product or the production costs of that product.

NEW QUESTION: 232
Which of the following is the MOST important objective of the information system control?
A. Business objectives are achieved and undesired risk events are detected and corrected
B. Ensuring effective and efficient operations
C. Developing business continuity and disaster recovery plans
D. Safeguarding assets
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:

The basic purpose of Information System control in an organization is to ensure that the business objectives are achieved and undesired risk events are detected and corrected. Some of the IS control objectives are given below:
* Safeguarding assets
* Assuring integrity of sensitive and critical application system environments
* Assuring integrity of general operating system
* Ensuring effective and efficient operations
* Fulfilling user requirements, organizational policies and procedures, and applicable laws and regulations
* Changing management
* Developing business continuity and disaster recovery plans
* Developing incident response and handling plans
Hence the most important objective is to ensure that business objectives are achieved and undesired risk events are detected and corrected.
Incorrect Answers:
B, C, D: These are also the objectives of the information system control but are not the best answer.

NEW QUESTION: 233
A change management process has recently been updated with new testing procedures. The NEXT course of action is to:
A. communicate to those who test and promote changes
B. assess the maturity of the change management process
C. conduct a cost-benefit analysis to justify the cost of the control
D. monitor processes to ensure recent updates are being followed
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 234
Which of the following controls do NOT come under technical class of control?
A. Program management control
B. System and Communications Protection control
C. Identification and Authentication control
D. Access Control
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Program Management control comes under management class of controls, not technical.
Program Management control is driven by the Federal Information Security Management Act (FISMA). It provides controls to ensure compliance with FISMA. These controls complement other controls. They don't replace them.

Incorrect Answers:
B, C, D: These controls comes under technical class of control.
The Technical class of controls includes four families. These families include over 75 individual controls.
Following is a list of each of the families in the Technical class:
Access Control (AC): This family of controls helps an organization implement effective access control.

- They ensure that users have the rights and permissions they need to perform their jobs, and no more. It includes principles such as least privilege and separation of duties.

Audit and Accountability (AU): This family of controls helps an organization implement an effective audit

- program. It provides details on how to determine what to audit. It provides details on how to protect the audit logs. It also includes information on using audit logs for non-repudiation.

Identification and Authentication (IA): These controls cover different practices to identify and

- authenticate users. Each user should be uniquely identified. In other words, each user has one account. This account is only used by one user. Similarly, device identifiers uniquely identify devices on the network.

System and Communications Protection (SC): The SC family is a large group of controls that cover

- many aspects of protecting systems and communication channels. Denial of service protection and boundary protection controls are included. Transmission integrity and confidentiality controls are also included.

NEW QUESTION: 235
Which of the following would be the BEST key performance indicator (KPI) for monitoring the effectiveness of the IT asset management process?
A. Percentage of unpatched IT assets
B. The number of IT assets procured during the previous month
C. The number of IT assets securely disposed during the past year
D. Percentage of IT assets without ownership
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 236
Which of the following is the BEST key performance indicator (KPI) for determining how well an IT policy is aligned to business requirements?
A. Total cost of policy breaches.
B. Total cost to support the policy.
C. Number of exceptions to the policy.
D. Number of inquiries regarding the policy.

Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 237
IT disaster recovery point objectives (RPOs) should be based on the:
A. type of business.
B. need of each business unit.
C. maximum tolerable loss of data.
D. maximum tolerable downtime.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 238
Which of the following is the way to verify control effectiveness?
A. The capability of providing notification of failure.
B. Whether it is preventive or detective.
C. Its reliability.
D. The test results of intended objectives.
E. Explanation:
Control effectiveness requires a process to verify that the control process worked as intended and meets the intended control objectives.
Hence the test result of intended objective helps in verifying effectiveness of control.
F. is incorrect. Reliability is not an indication of control strength; weak controls can be highly reliable, even if they do not meet the control objective.
G. is incorrect. The type of control, like preventive or detective, does not help determine control effectiveness.
Answer: (SHOW ANSWER)
is incorrect. Notification of failure does not determine control strength, hence this option is not correct.

NEW QUESTION: 239
Which of the following is the MOST important reason to maintain key risk indicators (KRIs)?
A. In order to avoid risk
B. Complex metrics require fine-tuning
C. Risk reports need to be timely
D. Threats and vulnerabilities change over time
E. Explanation:
Threats and vulnerabilities change over time and KRI maintenance ensures that KRIs continue to effectively capture these changes. The risk environment is highly dynamic as the enterprise's internal and external environments are constantly changing. Therefore, the set of KRIs needs to be changed over time, so that they can capture the changes in threat and vulnerability.
Answer: D,E (LEAVE A REPLY)

is incorrect. While most key risk indicator (KRI) metrics need to be optimized in respect to their sensitivity, the most important objective of KRI maintenance is to ensure that KRIs continue to effectively capture the changes in threats and vulnerabilities over time. Hence the most important reason is that because of change of threat and vulnerability overtime. Answer: C is incorrect. Risk reporting timeliness is a business requirement, but is not a reason for KRI maintenance. Answer: A is incorrect. Risk avoidance is one possible risk response. Risk responses are based on KRI reporting, but is not the reason for maintenance of KRIs.

NEW QUESTION: 240
Which of the following IT controls is MOST useful in mitigating the risk associated with inaccurate data?
A. Audit trails for updates and deletions
B. Encrypted storage of data
C. Links to source data
D. Check totals on data records and data fields
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 241
Which of the following process ensures that extracted data are ready for analysis?
A. Data analysis
B. Data validation
C. Data gathering
D. Data access
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Data validation ensures that extracted data are ready for analysis. One objective is to perform data quality tests to ensure data are valid complete and free of errors. This may also involve making data from different sources suitable for comparative analysis.
Incorrect Answers:
A: Analysis of data involves simple set of steps or complex combination of commands and other functionality. Data analysis is designed in such a way to achieve the stated objectives from the project plan. Although this may be applicable to any monitoring activity, it would be beneficial to consider transferability and scalability. This may include robust documentation, use of software development standards and naming conventions.
C: Data gathering is the process of collecting data on risk to be monitored, prepare a detailed plan and define the project's scope. In the case of a monitoring project, this step should involve process owners, data owners, system custodians and other process stakeholders.
D: In the data access process, management identifies which data are available and how they can be acquired in a format that can be used for analysis. There are two options for data extraction:

- Extracting data directly from the source systems after system owner approval
- Receiving data extracts from the system custodian (IT) after system owner approval

NEW QUESTION: 242
Which of the following is the GREATEST concern when using a generic set of IT risk scenarios for risk analysis?
A. Inherent risk might not be considered
B. Implementation costs might increase
C. Risk factors might not be relevant to the organization
D. Quantitative analysis might not be possible
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 243
Which of the following is MOST important to update when an organization's risk appetite changes?
A. Key risk indicators (KRIs)
B. Risk taxonomy
C. Key performance indicators (KPIs)
D. Risk reporting methodology
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 244
Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?
A. A quantitative presentation of risk assessment results
B. A qualitative presentation of risk assessment results
C. A comparison of risk assessment results to the desired state
D. An assessment of organizational maturity levels and readiness
Answer: (SHOW ANSWER)

Section: Volume D

NEW QUESTION: 245
Which of the following statements is NOT true regarding the risk management plan?
A. The risk management plan is an output of the Plan Risk Management process.
B. The risk management plan is an input to all the remaining risk-planning processes.
C. The risk management plan includes a description of the risk responses and triggers.
D. The risk management plan includes thresholds, scoring and interpretation methods, responsible parties, and budgets.
Answer: C (LEAVE A REPLY)
Section: Volume C
Explanation:
The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. The risk management plan does not include responses to risks or triggers. Responses to risks are documented in the risk register as part of the Plan Risk Responses process.
Incorrect Answers:
A, B, D: These all statements are true for risk management plan. The risk management plan details how risk management processes will be implemented, monitored, and controlled throughout the life of the project. It includes thresholds, scoring and interpretation methods, responsible parties, and budgets. It also acts as input to all the remaining risk-planning processes.

NEW QUESTION: 246
Mary is the project manager for the BLB project. She has instructed the project team to assemble, to review the risks. She has included the schedule management plan as an input for the quantitative risk analysis process. Why is the schedule management plan needed for quantitative risk analysis?
A. Mary will schedule when the identified risks are likely to happen and affect the project schedule.
B. Mary will utilize the schedule controls and the nature of the schedule for the quantitative analysis of the schedule.
C. Mary will use the schedule management plan to schedule the risk identification meetings throughout the remaining project.
D. Mary will utilize the schedule controls to determine how risks may be allowed to change the project schedule.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The controls within the schedule management plan can shape how quantitative risk analysis will be performed on the schedule.

Schedule management plan also describes how the schedule contingencies will be reported and assessed.
Incorrect Answers:
A: When risks are likely to happen is important, but it is not the best answer for this question C: This is not a valid answer for this question throughout the project, but it is not scheduled during the quantitative risk analysis process.
D: Risks may affect the project schedule, but this is not the best answer for the question.

NEW QUESTION: 247
You are the project manager of the GHY Project for your company. You need to complete a project management process that will be on the lookout for new risks, changing risks, and risks that are now outdated. Which project management process is responsible for these actions?
A. Risk planning
B. Risk monitoring and controlling
C. Risk identification
D. Risk analysis
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The risk monitoring and controlling is responsible for identifying new risks, determining the status of risks that may have changed, and determining which risks may be outdated in the project.
Incorrect Answers:
A: Risk planning creates the risk management plan and determines how risks will be identified, analyzed, monitored and controlled, and responded to.
C: Risk identification is a process that identifies risk events in the project.
D: Risk analysis helps determine the severity of the risk events, the risks' priority, and the probability and impact of risks.

NEW QUESTION: 248
An organization operates in a jurisdiction where heavy fines are imposed for leakage of customer data. Which of the following provides the BEST input to assess the inherent risk impact?
A. Number of customer records held
B. Number of databases that host customer data
C. Number of encrypted customer databases
D. Number of staff members having access to customer data
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 249
A risk heat map is MOST commonly used as part of an IT risk analysis to facilitate risk:
A. treatment.

B. assessment
C. communication.
D. identification.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 250
Whether the results of risk analyses should be presented in quantitative or qualitative terms should be based PRIMARILY on the:
A. results of the risk assessment.
B. requirements of management.
C. organizational risk tolerance
D. specific risk analysis framework being used.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
Which of the following is MOST useful when communicating risk to management?
A. Risk policy
B. Risk map
C. Maturity model
D. Audit report
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 252
You work as the project manager for Bluewell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decide, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project, what is likely to increase?
A. Human resource needs
B. Quality control concerns
C. Costs
D. Risks
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Fast tracking allows entire phases of the project to overlap and generally increases risks within the project.
Fast tracking is a technique for compressing project schedule. In fast tracking, phases are overlapped that would normally be done in sequence. It is shortening the project schedule without reducing the project scope.
Incorrect Answers:

A: Human resources are not affected by fast tracking in most scenarios.
B: Quality control concerns usually are not affected by fast tracking decisions.
C: Costs do not generally increase based on fast tracking decisions.

NEW QUESTION: 253
The MOST important reason to aggregate results from multiple risk assessments on interdependent information systems is to:
A. identify critical information systems
B. facilitate communication to senior management
C. establish overall impact to the organization
D. efficiently manage the scope of the assignment
Answer: (SHOW ANSWER)

NEW QUESTION: 254
You are a project manager for your organization and you're working with four of your key stakeholders. One of the stakeholders is confused as to why you're not discussing the current problem in the project during the risk identification meeting. Which one of the following statements best addresses when a project risk actually happens?
A. Project risks are uncertain as to when they will happen.
B. Risks can happen at any time in the project.
C. Project risks are always in the future.
D. Risk triggers are warning signs of when the risks will happen.
E. Explanation:
According to the PMBOK, a project risk is always in the future. If the risk event has already happened, then it is an issue, not a risk.
F. is incorrect. You can identify risks before they occur and not after their occurrence.
Answer: (SHOW ANSWER)
is incorrect. Triggers are warning signs and conditions of risk events, but this answer isn't the best choice for this option B is incorrect. Risks can only happen in the future.

NEW QUESTION: 255
Participants in a risk workshop have become focused on the financial cost to mitigate risk rather than choosing the most appropriate response. Which of the following is the BEST way to address this type of issue in the long term?
A. Perform a return on investment analysis.
B. Raise the maturity of organizational risk management.
C. Review the risk register and risk scenarios.
D. Calculate annualized loss expectancy of risk scenarios.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256

Which of the following is the PRIMARY reason to update a risk register with risk assessment results?

A. To communicate the level and priority of assessed risk to management

B. To enable the creation of action plans to address nsk

C. To assign a risk owner to manage the risk

D. To provide a comprehensive inventory of risk across the organization

Answer: (SHOW ANSWER)

NEW QUESTION: 257

FISMA requires federal agencies to protect IT systems and data. How often should compliance be audited by an external organization?

A. Annually

B. Quarterly

C. Every three years

D. Never

Answer: A (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Inspection of FISMA is required to be done annually. Each year, agencies must have an independent evaluation of their program. The objective is to determine the effectiveness of the program. These evaluations include:

Testing for effectiveness: Policies, procedures, and practices are to be tested. This evaluation does not

- test every policy, procedure, and practice. Instead, a representative sample is tested.

An assessment or report: This report identifies the agency's compliance as well as lists compliance with

- FISMA. It also lists compliance with other standards and guidelines.

Incorrect Answers:

B, C, D: Auditing of compliance by external organization is done annually, not quarterly or every three year.

NEW QUESTION: 258
Which of the following is MOST helpful in aligning IT risk with business objectives?
A. Introducing an approved IT governance framework
B. Integrating the results of top-down risk scenario analyses
C. Implementing a risk classification system
D. Performing a business impact analysis (BIA)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 259
After the review of a risk record, internal audit questioned why the risk was lowered from medium to low.
Which of the following is the BEST course of action in responding to this inquiry?
A. Reopen the risk issue and complete a full assessment.
B. Obtain industry benchmarks related to the specific risk.
C. Provide justification for the lower risk rating.
D. Notify the business at the next risk briefing.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 260
Which of the following is a KEY responsibility of the second line of defense?
A. Owning risk scenarios
B. Monitoring control effectiveness
C. Implementing control activities
D. Conducting control self-assessments
Answer: B (LEAVE A REPLY)

NEW QUESTION: 261
Which of the following BEST facilities the alignment of IT risk management with enterprise risk management (ERM)?
A. linking IT risk scenarios to enterprise strategy
B. Linking IT risk scenarios to technology objectives
C. Adopting qualitative enterprise risk assessment methods
D. Adopting quantitative enterprise risk assessment methods
Answer: (SHOW ANSWER)

NEW QUESTION: 262
Which of the following is the GREATEST concern associated with redundant data in an organization's inventory system?
A. Data inconsistency
B. Unnecessary data storage usage
C. Poor access control

D. Unnecessary costs of program changes
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 263
Which of the following is MOST important to understand when developing key risk indicators (KRIs)?
A. Stakeholder requirements
B. Integrity of the source data
C. KRI thresholds
D. Control environment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 264
Which of the following is the STRONGEST indication an organization has ethics management issues?
A. Employees face sanctions for not signing the organization's acceptable use policy.
B. The organization has only two lines of defense.
C. Internal IT auditors report to the chief information security officer (CISO).
D. Employees do not report IT risk issues for fear of consequences.
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 265
Which of the following is MOST useful when communicating risk to management?
A. Risk policy
B. Audit report
C. Risk map
D. Maturity model
Answer: A (LEAVE A REPLY)

NEW QUESTION: 266
Which of the following statements are true for risk communication? Each correct answer represents a complete solution. Choose three.
A. It requires a practical and deliberate scheduling approach to identify stakeholders, actions, and concerns.
B. It helps in allocating the information concerning risk among the decision-makers.
C. It requires investigation and interconnectivity of procedural, legal, social, political, and economic factors.
D. It defines the issue of what a stakeholder does, not just what it says.
Answer: A,C,D (LEAVE A REPLY)

Explanation/Reference:
Explanation:
Risk communication is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions. Risk communication is mostly concerned with the nature of risk or expressing concerns, views, or reactions to risk managers or institutional bodies for risk management. The key plan to consider and communicate risk is to categorize and impose priorities, and acquire suitable measures to reduce risks. It is important throughout any crisis to put across multifaceted information in a simple and clear manner.
Risk communication helps in switching or allocating the information concerning risk among the decision- maker and the stakeholders.
Risk communication can be explained more clearly with the help of the following definitions:
It defines the issue of what a group does, not just what it says.

- It must take into account the valuable element in user's perceptions of risk.
- It will be more valuable if it is thought of as conversation, not instruction.

Risk communication is a fundamental and continuing element of the risk analysis exercise, and the involvement of the stakeholder group is from the beginning. It makes the stakeholders conscious of the process at each phase of the risk assessment. It helps to guarantee that the restrictions, outcomes, consequence, logic, and risk assessment are undoubtedly understood by all the stakeholders.
Incorrect Answers:
B: It helps in allocating the information concerning risk not only among the decision-makers but also stakeholders.

NEW QUESTION: 267
Which of the following is an administrative control?
A. Data loss prevention program
B. Session timeout
C. Water detection
D. Reasonableness check
Answer: (SHOW ANSWER)

NEW QUESTION: 268
You are the project manager of GHT project. You have identified a risk event on your project that could save $100,000 in project costs if it occurs. Which of the following statements BEST describes this risk event?
A. This risk event should be mitigated to take advantage of the savings.
B. This is a risk event that should be accepted because the rewards outweigh the threat to the project.
C. This risk event should be avoided to take full advantage of the potential savings.
D. This risk event is an opportunity to the project and should be exploited.

E. Explanation:
This risk event has the potential to save money on project costs, so it is an opportunity, and the appropriate strategy to use in this case is the exploit strategy. The exploit response is one of the strategies to negate risks or threats appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.
Answer: D,E (LEAVE A REPLY)
is incorrect. To accept risk means that no action is taken relative to a particular risk; loss is accepted if it occurs. But as this risk event bring an opportunity, it should me exploited and not accepted. Answer: A and C are incorrect. Mitigation and avoidance risk response is used in case of negative risk events, and not in positive risk events. Here in this scenario, as it is stated that the event could save $100,000, hence it is a positive risk event. Therefore should not be mitigated or avoided.

NEW QUESTION: 269
What are the responsibilities of the CRO?
Each correct answer represents a complete solution. Choose three.
A. Managing the risk assessment process
B. Implement corrective actions
C. Advising Board of Directors
D. Managing the supporting risk management function
Answer: A,B,D (LEAVE A REPLY)
Chief Risk Officer is the executive-level manager in an organization. They provide corporate, guidance, governance, and oversight over the enterprise's risk management activities. The main priority for the CRO is to ensure that the organization is in full compliance with applicable regulations. They may also deal with areas regarding insurance, internal auditing, corporate investigations, fraud, and information security. CRO's responsibilities include: Managing the risk assessment process Implementation of corrective actions Communicate risk management issues Supporting the risk management functions

NEW QUESTION: 270
An organization outsources the processing of us payroll data A risk practitioner identifies a control weakness at the third party trial exposes the payroll dat a. Who should own this risk?
A. The organization's process owner
B. The organization's risk practitioner
C. The third party's IT operations manager
D. The third party's chief risk officer (CRO)
Answer: (SHOW ANSWER)

NEW QUESTION: 271
IT management has asked for a consolidated view into the organization's risk profile to enable project prioritization and resource allocation. Which of the following materials would be MOST helpful?
A. List of key risk indicators
B. Internal audit reports
C. IT risk register
D. List of approved projects
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 272
Which of the following are the MOST important risk components that must be communicated among all the stakeholders?
Each correct answer represents a part of the solution. Choose three.
A. Various risk response used in the project
B. Expectations from risk management
C. Current risk management capability
D. Status of risk with regard to IT risk
Answer: B,C,D (LEAVE A REPLY)
Section: Volume C
Explanation:
The broad array of information and the major types of IT risk information that should be communicated are as follows:
* Expectations from risk management: They include risk strategy, policies, procedures, awareness training, uninterrupted reinforcement of principles, etc. This essential communication drives all subsequent efforts on risk management and sets the overall expectations from risk management.
* Current risk management capability: This allows monitoring of the status of the risk management engine in the enterprise. It is a key indicator for effective risk management and has predictive value for how well the enterprise is managing risk and reducing exposure.

* Status with regard to IT risk: This describes the actual status with regard to IT risk including information of risk profile of the enterprise, Key risk indicators (KRIs) to support management reporting on risk, event-loss data, root cause of loss events and options to mitigate risk.
Incorrect Answers:
A: Risk response is only communicated to some of the stakeholders not all, as it is irrelevant for them. It is not communicated to the stakeholders of the project like project sponsors, etc.

NEW QUESTION: 273
Which of The following will BEST communicate the importance of risk mitigation initiatives to senior management?
A. Balanced scorecard
B. Business case
C. Heat map
D. Industry standards
Answer: B (LEAVE A REPLY)

NEW QUESTION: 274
You are the project manager of a project in Bluewell Inc. You and your project team have identified several project risks, completed risk analysis, and are planning to apply most appropriate risk responses. Which of the following tools would you use to choose the appropriate risk response?
A. Project network diagrams
B. Cause-and-effect analysis
C. Decision tree analysis
D. Delphi Technique
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Decision tree analysis is a risk analysis tool that can help the project manager in determining the best risk response. The tool can be used to measure probability, impact, and risk exposure and how the selected risk response can affect the probability and/or impact of the selected risk event. It helps to form a balanced image of the risks and opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.
Incorrect Answers:
A: Project network diagrams help the project manager and stakeholders visualize the flow of the project work, but they are not used as a part of risk response planning.
B: Cause-and-effect analysis is used for exposing risk factors and not an effective one in risk response planning.

This analysis involves the use of predictive or diagnostic analytical tool for exploring the root causes or factors that contribute to positive or negative effects or outcomes.
D: Delphi technique is used for risk analysis, i.e., for identifying the most probable risks. Delphi is a group of experts who used to rate independently the business risk of an organization. Each expert analyzes the risk independently and then prioritizes the risk, and the result is combined into a consensus.

NEW QUESTION: 275
Management has noticed storage costs have increased exponentially over the last 10 years because most users do not delete their emails. Which of the following can BEST alleviate this issue while not sacrificing security?
A. Implementing record retention tools and techniques
B. Implementing a bring your own device 1BVOD) policy
C. Establishing e-discovery and data loss prevention (DLP)
D. Sending notifications when near storage quota
Answer: A (LEAVE A REPLY)

NEW QUESTION: 276
Shawn is the project manager of the HWT project. In this project Shawn's team reports that they have found a way to complete the project work cheaply than what was originally estimated earlier. The project team presents a new software that will help to automate the project work. While the software and the associated training costs $25,000 it will save the project nearly $65,000 in total costs. Shawn agrees to the software and changes the project management plan accordingly. What type of risk response had been used by him?
A. Avoiding
B. Accepting
C. Exploiting
D. Enhancing
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
A risk event is being exploited so as to identify the opportunities for positive impacts. Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized.
Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.
Incorrect Answers:
A: To avoid a risk means to evade it altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event.

B: Accepting is a risk response that is appropriate for positive or negative risk events. It does not pursue the risk, but documents the event and allows the risk to happen. Often acceptance is used for low probability and low impact risk events.
D: Enhancing is a positive risk response that aims to increase the probability and/or impact of the risk event.

NEW QUESTION: 277
A risk practitioner has discovered a deficiency in a critical system that cannot be patched. Which of the following should be the risk practitioner's FIRST course of action?
A. Review the business impact assessment.
B. Submit a request to change management.
C. Report the issue to internal audit.
D. Conduct a risk assessment.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 278
Which of the following is the BEST method to identify unnecessary controls?
A. Evaluating existing controls against audit requirements
B. Evaluating the impact of removing existing controls
C. Reviewing system functionalities associated with business processes
D. Monitoring existing key risk indicators (KRIs)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 279
Sammy is the project manager for her organization. She would like to rate each risk based on its probability and affect on time, cost, and scope. Harry, a project team member, has never done this before and thinks Sammy is wrong to attempt this approach. Harry says that an accumulative risk score should be created, not three separate risk scores. Who is correct in this scenario?
A. Sammy is correct, because she is the project manager.
B. Sammy is correct, because organizations can create risk scores for each objective of the project.
C. Harry is correct, the risk probability and impact matrix is the only approach to risk assessment.
D. Harry is correct, because the risk probability and impact considers all objectives of the project.
E. Explanation:
Sammy She certainly can create an assessment for a risk event for time cost, and scope. It is probable that a risk event may have an effect on just one or more objectives so an assessment of the objective is acceptable.
Answer: B (LEAVE A REPLY)
is incorrect. Just because Sammy is the project manager, it is not necessary that she is right.
Answer:D is incorrect. Harry's reasoning is flawed as each objective can be reviewed for the risk's

impact rather than the total project. Answer:C is incorrect. Harry is incorrect as there are multiple approaches to risk assessment for a project

NEW QUESTION: 280
An organization has allowed its cyber risk insurance to lapse while seeking a new insurance provider. The risk practitioner should report to management that the risk has been:
A. accepted
B. mitigated
C. transferred
D. avoided
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 281
Which of the following would BEST help to ensure that identified risk is efficiently managed?
A. Reviewing the maturity of the control environment
B. Maintaining a key risk indicator for each asset in the risk register
C. Regularly monitoring the project plan
D. Periodically reviewing controls per the risk treatment plan
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 282
You are the project manager of GHT project. You have implemented an automated tool to analyze and report on access control logs based on severity. This tool generates excessively large amounts of results. You perform a risk assessment and decide to configure the monitoring tool to report only when the alerts are marked "critical". What you should do in order to fulfill that?
A. Apply risk response
B. Optimize Key Risk Indicator
C. Update risk register
D. Perform quantitative risk analysis
Answer: B (LEAVE A REPLY)
Section: Volume B
Explanation:
As the sensitivity of the monitoring tool has to be changed, therefore it requires optimization of Key Risk Indicator. The monitoring tool which is giving alerts is itself acting as a risk indicator. Hence to change the sensitivity of the monitoring tool to give alert only for critical situations requires optimization of the KRI.
Incorrect Answers:
A, C, D: These options are not relevant to the change of sensitivity of the monitoring tools.

NEW QUESTION: 283
Which of the following is the MOST effective method for indicating that the risk level is approaching a high or unacceptable level of risk?
A. Risk register
B. Cause and effect diagram
C. Risk indicator
D. Return on investment
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:
Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Incorrect Answers:
A: A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:
* A description of the risk
* The impact should this event actually occur
* The probability of its occurrence
* Risk Score (the multiplication of Probability and Impact)
* A summary of the planned response should the event occur
* A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event)
* Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved.
D: Return On Investment (ROI) is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments. To calculate ROI, the benefit (return) of an investment is divided by the cost of the investment; the result is expressed as a percentage or a ratio.
The return on investment formula:
ROI= (Gain from investment - Cost of investment) / Cost of investment
In the above formula "gains from investment", refers to the proceeds obtained from selling the investment of interest.

NEW QUESTION: 284
Courtney is the project manager for her organization. She is working with the project team to complete the qualitative risk analysis for her project. During the analysis Courtney encourages the project team to begin the grouping of identified risks by common causes. What is the primary advantage to group risks by common causes during qualitative risk analysis?
A. It helps the project team realize the areas of the project most laden with risks.
B. It assist in developing effective risk responses.

C. It saves time by collecting the related resources, such as project team members, to analyze the risk events.
D. It can lead to the creation of risk categories unique to each project.
Answer: B (LEAVE A REPLY)
By grouping the risks by categories the project team can develop effective risk responses. Related risk events often have common causal factors that can be addressed with a single risk response.

NEW QUESTION: 285
You are the project manager of your enterprise. You have identified several risks. Which of the following responses to risk is considered the MOST appropriate?
A. Any of the above
B. Insuring
C. Avoiding
D. Accepting
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation:
The appropriate response to the risk is decided by the risk itself, the company's attitude and appetite of risk, and the threat and opportunity combination of the risk.
Incorrect Answers:
B, C, D: Depending upon the condition, that is, the risk itself, the company's attitude and appetite of risk, and the threat and opportunity combination of the risk, these response options can be chosen.

NEW QUESTION: 286
An organization operates in an environment where reduced time-to-market for new software products is a top business priority. Which of the following should be the risk practitioner's GREATEST concern?
A. Email infrastructure does not have proper rollback plans
B. Sufficient resources are not assigned to IT development projects
C. The corporate email system does not identify and store phishing emails
D. Customer support help desk staff does not have adequate training
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 287
Which of the following is the HIGHEST risk of a policy that inadequately defines data and system ownership?
A. User management coordination does not exist
B. Audit recommendations may not be implemented
C. Users may have unauthorized access to originate, modify or delete data
D. Specific user accountability cannot be established
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
There is an increased risk without a policy defining who has the responsibility for granting access to specific data or systems, as one could gain system access without a justified business needs. There is better chance that business objectives will be properly supported when there is appropriate ownership.
Incorrect Answers:
A, B, D: These risks are not such significant as compared to unauthorized access.

NEW QUESTION: 288
Which of the following decision tree nodes have probability attached to their branches?
A. Root node
B. Event node
C. End node
D. Decision node
Answer: (SHOW ANSWER)
Section: Volume B
Explanation:
Event nodes represents the possible uncertain outcomes of a risky decision, with at least two nodes to illustrate the positive and negative range of events. Probabilities are always attached to the branches of event nodes.
Incorrect Answers:
A: Root node is the starting node in the decision tree, and it has no branches.
C: End node represents the outcomes of risk and decisions and probability is not attached to it.
D: It represents the choice available to the decision maker, usually between a risky choice and its non-risky counterpart. As it represents only the choices available to the decision makers, hence probability is not attached to it.

NEW QUESTION: 289

In which of the following risk management capability maturity levels does the enterprise takes major business decisions considering the probability of loss and the probability of reward? Each correct answer represents a complete solution. Choose two.

A. Level 0

B. Level 2

C. Level 5

D. Level 4

Answer: C,D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Enterprise having risk management capability maturity level 4 and 5 takes business decisions considering the probability of loss and the probability of reward, i.e., considering all the aspects of risk.

Incorrect Answers:

A: Enterprise having risk management capability maturity level 0 takes business decisions without considering risk credential information.

B: At this low level of risk management capability the enterprise take decisions considering specific risk issues within functional and business silos (e.g., security, business continuity, operations).

NEW QUESTION: 290

Which of the following should be implemented to BEST mitigate the risk associated with infrastructure updates?

A. Change management audit

B. Change control process

C. Role-specific technical training

D. Risk assessment

Answer: (SHOW ANSWER)

NEW QUESTION: 291

While defining the risk management strategies, what are the major parts to be determined first? Each correct answer represents a part of the solution. Choose two.

A. IT architecture complexity

B. Organizational objectives

C. Risk tolerance

D. Risk assessment criteria

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

While defining the risk management strategies, risk professional should first identify and analyze the objectives of the organization and the risk tolerance. Once the objectives of enterprise are

known, risk professional can detect the possible risks which can occur in accomplishing those objectives. Analyzing the risk tolerance would help in identifying the priorities of risk which is the latter steps in risk management.
Hence these two do the basic framework in risk management.
Incorrect Answers:
A: IT architecture complexity is related to the risk assessment and not the risk management, as it does much help in evaluating each significant risk identified.
D: Risk assessment is one of the various phases that occur while managing risks, which uses quantitative and qualitative approach to evaluate risks. Hence risk assessment criteria is only a part of this framework.

NEW QUESTION: 292
Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?
A. Business Continuity Strategy
B. Index of Disaster-Relevant Information
C. Disaster Invocation Guideline
D. Availability/ ITSCM/ Security Testing Schedule
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:
The Business Continuity Strategy is an outline of the approach to ensure the continuity of Vital Business Functions in the case of disaster events. The Business Continuity Strategy is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy.
Incorrect Answers:
B: Index of Disaster-Relevant Information is a catalog of all information that is relevant in the event of disasters.
This document is maintained and circulated by IT Service Continuity Management to all members of IT staff with responsibilities for fighting disasters.
C: Disaster Invocation Guideline is a document produced by IT Service Continuity Management with detailed instructions on when and how to invoke the procedure for fighting a disaster. Most importantly, the guideline defines the first step to be taken by the Service Desk after learning that a disaster has occurred.
D: Availability/ ITSCM/ Security Testing Schedule is a schedule for the regular testing of all availability, continuity, and security mechanisms jointly maintained by Availability, IT Service Continuity, and IT Security Management.

NEW QUESTION: 293
You work as a project manager for Bluewell Inc. You have identified a project risk. You have then implemented the risk action plan and it turn out to be non-effective. What type of plan you should implement in such case?

A. Risk mitigation
B. Risk fallback plan
C. Risk avoidance
D. Risk response plan
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A risk fallback plan is a proper plan devised to identify definite action to be taken if the risk action plan (Risk Mitigation Plan) is not helpful. Fallback plan is important in Risk Response Planning. If the contingency plan for a risk is not successful, then the project team implements the fallback plan. Fall-back planning is intended for a known and specific activity that may perhaps fail to produce desired outcome. It is related with technical procedures and with the responsibility of the technical lead.
Incorrect Answers:
A, C, D: These all choices itself comes under risk action plan. As in the described scenario, risk action plan is not turned to be effective, these should not be implemented again.

NEW QUESTION: 294
A global company s business continuity plan (BCP) requires the transfer of its customer information....
event of a disaster. Which of the following should be the MOST important risk consideration?
A. The organizational culture differences between each country
B. The lack of a service level agreement (SLA) in the vendor contract
C. The difference In the management practices between each company
D. The cloud computing environment is shared with another company
Answer: D (LEAVE A REPLY)

NEW QUESTION: 295
You are the project manager of GHT project. You have planned the risk response process and now you are about to implement various controls. What you should do before relying on any of the controls?
A. Review performance data
B. Discover risk exposure
C. Conduct pilot testing
D. Articulate risk
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:
Pilot testing and reviewing of performance data to verify operation against design are done before relying on control.
Incorrect Answers:

B: Discovering risk exposure helps in identifying the severity of risk, but it does not play any role in specifying the reliability of control.
D: Articulating risk is the first phase in the risk response process to ensure that information on the true state of exposures and opportunities are made available in a timely manner and to the right people for appropriate response. But it does not play any role in identifying whether any specific control is reliable or not.

NEW QUESTION: 296
Kelly is the project manager of the NNQ Project for her company. This project will last for one year and has a budget of $350,000. Kelly is working with her project team and subject matter experts to begin the risk response planning process. What are the two inputs that Kelly would need to begin the plan risk response process?
A. Risk register and the results of risk analysis
B. Risk register and the risk response plan
C. Risk register and power to assign risk responses
D. Risk register and the risk management plan
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The only two inputs for the risk response planning are the risk register and the risk management plan.
The plan risk response project management process aims to reduce the threats to the project objectives and to increase opportunities. It follows the perform qualitative risk analysis process and perform quantitative risk analysis process. Plan risk response process includes the risk response owner to take the job for each agreed-to and funded risk response. This process addresses the risks by their priorities, schedules the project management plan as required, and inserts resources and activities into the budget.
The inputs to the plan risk response process are as follows:
Risk register
- Risk management plan

Incorrect Answers:
B: Kelly will not need the risk response plan until monitoring and controlling the project.
C: The results of risk analysis will help Kelly prioritize the risks, but this information will be recorded in the risk register.
D: Kelly needs the risk register and the risk management plan as the input. The power to assign risk responses is not necessarily needed by Kelly.

NEW QUESTION: 297
A control owner has completed a year-long project To strengthen existing controls. It is MOST important for the risk practitioner to:

A. ensure risk monitoring for the project is initiated.
B. update the risk register to reflect the correct level of residual risk.
C. conduct and document a business impact analysis (BIA).
D. verify cost-benefit of the new controls betng implemented.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 298
Periodically reviewing and updating a risk register with details on identified risk factors PRIMARILY helps to:
A. provide a current reference to stakeholders for risk-based decisions
B. minimize the number of risk scenarios for risk assessment
C. aggregate risk scenarios identified across different business units
D. build a threat profile of the organization for management review
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 299
Which of the following BEST indicates that additional or improved controls ate needed m the environment?
A. Management, has decreased organisational risk appetite
B. merging risk scenarios have been identified
C. The risk register and portfolio do not include all risk scenarios
D. Risk events and losses exceed risk tolerance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 300
Which element of an organization's risk register is MOST important to update following the commissioning of a new financial reporting system?
A. The risk rating of affected financial processes
B. Key risk indicators (KRIs)
C. The owner of the financial reporting process
D. The list of relevant financial controls
Answer: (SHOW ANSWER)

NEW QUESTION: 301
An organization has outsourced its lease payment process to a service provider who lacks evidence of compliance with a necessary regulatory standard. Which risk treatment was adopted by the organization?
A. Avoidance
B. Mitigation
C. Transfer

D. Acceptance
Answer: (SHOW ANSWER)

NEW QUESTION: 302
Which of the following BEST indicates the condition of a risk management program?
A. Number of controls
B. Number of risk register entries
C. Amount of residual risk
D. Level of financial support
Answer: C (LEAVE A REPLY)

NEW QUESTION: 303
Jeff works as a Project Manager for www.company.com Inc. He and his team members are involved in the identify risk process. Which of the following tools & techniques will Jeff use in the identify risk process?
Each correct answer represents a complete solution. (Choose three.)
A. Information gathering technique
B. Documentation reviews
C. Checklist analysis
D. Risk categorization
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The various tools & techniques used in the identify risk process are as follows:
Documentation reviews
- Information gathering technique
- Checklist analysis
- Assumption analysis
- Diagramming techniques
- SWOT analysis

Expert judgment

NEW QUESTION: 304
Which of the following are risk components of the COSO ERM framework?
Each correct answer represents a complete solution. Choose three.
A. Risk response
B. Internal environment
C. Business continuity
D. Control activities
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The risk components defined by the COSO ERM are internal environment, objective settings, event identification, risk assessment, risk response, control objectives, information and communication, and monitoring.
Incorrect Answers:
C: Business continuity is not considered as risk component within the ERM framework.

NEW QUESTION: 305
Risks to an organization's image are referred to as what kind of risk?
A. Operational
B. Financial
C. Information
D. Strategic
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Strategic risks are those risks which have potential outcome of not fulfilling on strategic objectives of the organization as planned. Since the strategic objective will shape and impact the entire organization, the risk of not meeting that objective can impose a great threat on the organization.
Strategic risks can be broken down into external and internal risks:
External risks are those circumstances from outside the enterprise which will have a potentially damaging or helpful impact on the enterprise. These risks include sudden change of economy, industry, or regulatory conditions. Some of the external risks are predictable while others are not. For instance, a recession may be predictable and the enterprise may be able to hedge against the dangers economically; but the total market failure may not as predictable and can be much more devastating.
Internal risks usually focus on the image or reputation of the enterprise. some of the risks that are involved in this are public communication, trust, and strategic agreement from stakeholders and customers.

NEW QUESTION: 306
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?
A. Develop an access control policy.
B. Perform root cause analysis.
C. Disable user access.
D. Perform a risk assessment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 307
Your project spans the entire organization. You would like to assess the risk of your project but worried about that some of the managers involved in the project could affect the outcome of any risk identification meeting.
Your consideration is based on the fact that some employees would not want to publicly identify risk events that could declare their supervision as poor. You would like a method that would allow participants to anonymously identify risk events. What risk identification method could you use?
A. Delphi technique
B. Root cause analysis
C. Isolated pilot groups
D. SWOT analysis
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:
The Delphi technique uses rounds of anonymous surveys to build consensus on project risks. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a question and their inputs are organized according to their contents. The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly.
Incorrect Answers:
B: Root cause analysis is not an anonymous approach to risk identification.
C: Isolated pilot groups is not a valid risk identification activity.
D: SWOT analysis evaluates the strengths, weaknesses, opportunities, and threats of the project.

NEW QUESTION: 308
Which of the following is the BEST key performance indicator (KPI) to measure the effectiveness of a vulnerability management process?
A. Percentage of vulnerabilities remediated within the agreed service level
B. Number of vulnerabilities identified during the period

C. Number of vulnerabilities re-opened during the period
D. Percentage of vulnerabilities escalated to senior management
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 309
What are the PRIMARY requirements for developing risk scenarios?
Each correct answer represents a part of the solution. Choose two.
A. Potential threats and vulnerabilities that could lead to loss events
B. Determination of the value of an asset at risk
C. Determination of actors that has potential to generate risk
D. Determination of threat type
Answer: A,B (LEAVE A REPLY)
Section: Volume A
Explanation:
Creating a scenario requires determination of the value of an asset or a business process at risk and the potential threats and vulnerabilities that could cause loss. The risk scenario should be assessed for relevance and realism, and then entered into the risk register if found to be relevant.
In practice following steps are involved in risk scenario development:
* First determine manageable set of scenarios, which include:
* Frequently occurring scenarios in the industry or product area.
* Scenarios representing threat sources that are increasing in count or severity level.
* Scenarios involving legal and regulatory requirements applicable to the business.
* After determining manageable risk scenarios, perform a validation against the business objectives of the entity.
* Based on this validation, refine the selected scenarios and then detail them to a level in line with the criticality of the entity.
* Lower down the number of scenarios to a manageable set. Manageable does not signify a fixed number, but should be in line with the overall importance and criticality of the unit.
* Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
* Risk factors kept in a register so that they can be reevaluated in the next iteration and included for detailed analysis if they have become relevant at that time.
* Include an unspecified event in the scenarios, that is, address an incident not covered by other scenarios.
Incorrect Answers:
C, D: Determination of actors and threat type are not the primary requirements for developing risk scenarios, but are the components that are determined during risk scenario development.

NEW QUESTION: 310

An organization has provided legal text explaining the rights and expected behavior of users accessing a system from geographic locations that have strong privacy regulations. Which of the following control types has been applied?

A. Preventive

B. Detective

C. Compensating

D. Directive

Answer: D (LEAVE A REPLY)

NEW QUESTION: 311

During which of the following processes, probability and impact matrix are prepared?

A. Risk response

B. Monitoring and Control Risk

C. Quantitative risk assessment

D. Qualitative risk assessment

E. Explanation:

The probability and impact matrix is a technique to prioritize identified risks of the project on their risk rating, and are being prepared while performing qualitative risk analysis. Evaluation of each risk's importance and, hence, priority for attention, is typically conducted using a look-up table or a probability and impact matrix. This matrix specifies combinations of probability and impact that lead to rating the risks as low, moderate, or high priority.

Answer: D,E (LEAVE A REPLY)

is incorrect. SLE, ARO and ALE are used in quantitative risk assessment. Answer:A and B are incorrect. These processes are part of Risk Management. The probability and impact matrix is prepared during the qualitative risk analysis for further quantitative analysis and response based on their risk rating.

NEW QUESTION: 312

Which of the following activities would BEST contribute to promoting an organization-wide risk-aware culture?

A. Communicating components of risk and their acceptable levels

B. Performing a benchmark analysis and evaluating gaps

C. Participating in peer reviews and implementing best practices

D. Conducting risk assessments and implementing controls

Answer: D (LEAVE A REPLY)

Section: Volume D

Explanation/Reference:

Reference: https://m.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/ Documents/CRISC-Additional-Verification-Form-2015-Later-frm_Eng_0818.pdf

NEW QUESTION: 313

Which of the following role carriers are responsible for setting up the risk governance process, establishing and maintaining a common risk view, making risk-aware business decisions, and setting the enterprise's risk culture?
Each correct answer represents a complete solution. Choose two.
A. Senior management
B. Chief financial officer (CFO)
C. Human resources (HR)
D. Board of directors
E. Explanation:
The board of directors and senior management has the responsibility to set up the risk governance process, establish and maintain a common risk view, make risk-aware business decisions, and set the enterprise's risk culture.
Answer: A,D,E (LEAVE A REPLY)
is incorrect. CFO is the most senior official 0f the enterprise who is accountable for financial planning, record keeping, investor relations and financial risks. CFO is not responsible for responsible for setting up the risk governance process, establishing and maintaining a common risk view, making risk-aware business decisions, and setting the enterprise's risk culture. Answer: C is incorrect. Human resource is the most senior official of an enterprise who is accountable for planning and policies with respect to all human resources in that enterprise. HR is not responsible for risk related activities.

NEW QUESTION: 314
You are the project manager of HGT project. You have identified project risks and applied appropriate response for its mitigation. You noticed a risk generated as a result of applying response. What this resulting risk is known as?
A. Pure risk
B. Secondary risk
C. Response risk
D. High risk
Answer: (SHOW ANSWER)
Section: Volume B
Explanation:
Secondary risk is a risk that is generated as the result of risk response.
Incorrect Answers:
A: A pure risk is a risk that has only a negative effect on the project. Pure risks are activities that are dangerous to complete and manage such as construction, electrical work, or manufacturing.
C, D: These terms are not applied for the risk that is generated as a result of risk response.

NEW QUESTION: 315
When developing a risk awareness training program, which of the following training topics would BEST facilitate a thorough understanding of risk scenarios?

A. Mapping threats to organizational objectives
B. Analyzing key risk indicators (KRIs)
C. Identifying potential sources of risk
D. Reviewing past audits
Answer: (SHOW ANSWER)

NEW QUESTION: 316
A recent risk workshop has identified risk owners and responses for newly identified risk scenarios. Which of the following should be the risk practitioner's NEXT step?
A. Prepare a business case for the response options.
B. Update the risk register with the results.
C. Develop a mechanism for monitoring residual risk.
D. Identify resources for implementing responses.
Answer: (SHOW ANSWER)

NEW QUESTION: 317
The BEST metric to monitor the risk associated with changes deployed to production is the percentage of:
A. changes due to emergencies.
B. personnel that have rights to make changes in production.
C. changes not requiring user acceptance testing.
D. changes that cause incidents.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 318
Which of The following is the MOST relevant information to include in a risk management strategy?
A. Regulatory requirements
B. Cost of controls
C. Quantified risk triggers
D. Organizational goals
Answer: A (LEAVE A REPLY)

NEW QUESTION: 319
The MOST effective way to increase the likelihood that risk responses will be implemented is to:
A. review progress reports
B. create an action plan
C. perform regular audits
D. assign ownership
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 320
Which of the following would present the GREATEST challenge when assigning accountability for control ownership?
A. Senior management scrutiny
B. Complex regulatory environment
C. Unclear reporting relationships
D. Weak governance structures
Answer: (SHOW ANSWER)

NEW QUESTION: 321
Employees are repeatedly seen holding the door open for others, so that trailing employees do not have to stop and swipe their own ID badges. This behavior BEST represents:
A. a threat.
B. a vulnerability.
C. an impact
D. a control.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 322
You are working as a project manager in Bluewell Inc.. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?
A. Qualitative risk analysis
B. Risk audits
C. Quantitative risk analysis
D. Requested changes
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Of all the choices given, only requested changes is an output of the monitor and control risks process. You might also have risk register updates, recommended corrective and preventive actions, organizational process assets, and updates to the project management plan.
Incorrect Answers:
A, C: These are the plan risk management processes.
B: Risk audit is a risk monitoring and control technique.

NEW QUESTION: 323
What is the IMMEDIATE step after defining set of risk scenarios?
A. Risk mitigation
B. Risk monitoring
C. Risk management
D. Risk analysis
E. Explanation:
Once the set of risk scenarios is defined, it can be used for risk analysis. In risk analysis, likelihood and impact of the scenarios are assessed. Important components of this assessment are the risk factors.
Answer: D,E (LEAVE A REPLY)
is incorrect. Risk analysis comes under risk management, therefore management is a generalized term, and is not the best answer for this B is incorrect. Risk monitoring is the latter step after risk analysis and risk mitigation. Answer: A is incorrect. Risk mitigation is the latter step after analyzing risk.

NEW QUESTION: 324
From a risk management perspective, the PRIMARY objective of using maturity models is to enable:
A. solution delivery
B. strategic alignment
C. resource utilization
D. performance evaluation
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 325
The FIRST step for a startup company when developing a disaster recovery plan should be to identify:
A. current vulnerabilities
B. a suitable alternate site
C. recovery time objectives
D. critical business processes
Answer: D (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 326
Which of The following is the MOST relevant information to include in a risk management strategy?
A. Cost of controls
B. Regulatory requirements
C. Organizational goals
D. Quantified risk triggers
Answer: (SHOW ANSWER)

NEW QUESTION: 327
Who is at the BEST authority to develop the priorities and identify what risks and impacts would occur if there were loss of the organization's private information?
A. External regulatory agencies
B. Internal auditor
C. Business process owners
D. Security management
E. Explanation:
Business process owners are in best position to judge the risks and impact, as they are most knowledgeable concerning their systems. Hence they are most suitable for developing and identifying risks on business.
Answer: (SHOW ANSWER)
D, and A are incorrect. Internal auditors, security managers, external regulators would not understand the impact on business to the extent that business owners could. Hence business owner is the best authority.

NEW QUESTION: 328
Which of the following BEST ensures that a firewall is configured in compliance with an enterprise's security policy?
A. Interview the firewall administrator.
B. Review the actual procedures.
C. Review the device's log file for recent attacks.
D. Review the parameter settings.
Answer: D (LEAVE A REPLY)
Section: Volume C
Explanation:
A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide reliable audit evidence documentation.
Incorrect Answers:

A: While interviewing the firewall administrator may provide a good process overview, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.
B: While procedures may provide a good understanding of how the firewall is supposed to be managed, they do not reliably confirm that the firewall configuration complies with the enterprise's security policy.
C: While reviewing the device's log file for recent attacks may provide indirect evidence about the fact that logging is enabled, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

NEW QUESTION: 329
An organization's control environment is MOST effective when
A. controls operate efficiently.
B. control designs are reviewed periodically
C. controls are implemented consistent
D. controls perform as intended.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 330
You are the project manager of GHT project. Your project utilizes a machine for production of goods. This machine has the specification that if its temperature would rise above 450 degree Fahrenheit then it may result in burning of windings. So, there is an alarm which blows when machine's temperature reaches 430 degree Fahrenheit and the machine is shut off for 1 hour. What role does alarm contribute here?
A. Of risk indicator
B. Of risk identification
C. Of risk trigger
D. Of risk response
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:
Explanation:
Here in this scenario alarm indicates the potential risk that the rising temperature of machine can cause, hence it is enacting as a risk indicator.
Risk indicators are metrics used to indicate risk thresholds, i.e., it gives indication when a risk level is approaching a high or unacceptable level of risk. The main objective of a risk indicator is to ensure tracking and reporting mechanisms that alert staff about the potential risks.
Incorrect Answers:
B: The first thing we must do in risk management is to identify the areas of the project where the risks can occur. This is termed as risk identification. Listing all the possible risks is proved to be very productive for the enterprise as we can cure them before it can occur. In risk identification both threats and opportunities are considered, as both carry some level of risk with them.

C: The temperature 430 degrees in scenario is the risk trigger. A risk trigger is a warning sign or condition that a risk event is about to happen. As in this scenario the 430-degree temperature is the indication of upcoming risks, hence 430 degree temperature is a risk trigger.
D: Risk response is the action taken to reduce the risk event occurrence. Hence here risk response is shutting off of machine.

NEW QUESTION: 331
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Alpha	High	Medium	High
Bravo	High	Low	Medium
Charlie	High	High	High
Delta	High	Medium	Medium

A. Project Delta
B. Project Bravo
C. Project Charlie
D. Project Alpha
Answer: C (LEAVE A REPLY)

NEW QUESTION: 332
You are working in an enterprise. You project deals with important files that are stored on the computer. You have identified the risk of the failure of operations. To address this risk of failure, you have guided the system administrator sign off on the daily backup. This scenario is an example of which of the following?
A. Risk avoidance
B. Risk transference
C. Risk acceptance
D. Risk mitigation
Answer: (SHOW ANSWER)

Section: Volume B
Explanation:
Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Here in this scenario, you are trying to reduce the risk of operation failure by guiding administrator to take daily backup, hence it is risk mitigation.
Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. The main control types are:
* Managerial(e.g.,policies)
* Technical (e.g., tools such as firewalls and intrusion detection systems)
* Operational (e.g., procedures, separation of duties)
* Preparedness activities
Incorrect Answers:
A: The scenario does not describe risk avoidance. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk.
B: The scenario does not describe the sharing of risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage.
C: The scenario does not describe risk acceptance, Acceptance is a strategy that provides for formal acknowledgment of the existence of a risk and the monitoring of that risk.

NEW QUESTION: 333
An organization is considering outsourcing user administration controls for a critical system. The potential vendor has offered to perform quarterly self-audits of its controls instead of having annual independent audits.
Which of the following should be of GREATEST concern to the risk practitioner?
A. The vendor will not achieve best practices
B. The vendor will not ensure against control failure
C. The controls may not be properly tested
D. Lack of a risk-based approach to access control
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 334
Qualitative risk assessment uses which of the following terms for evaluating risk level?
Each correct answer represents a part of the solution. Choose two.
A. Impact
B. Annual rate of occurrence
C. Probability
D. Single loss expectancy
Answer: (SHOW ANSWER)
Explanation/Reference:

Explanation:
Unlike the quantitative risk assessment, qualitative risk assessment does not assign dollar values. Rather, it determines risk's level based on the probability and impact of a risk. These values are determined by gathering the opinions of experts.
Probability- establishing the likelihood of occurrence and reoccurrence of specific risks, independently,
and combined. The risk occurs when a threat exploits vulnerability. Scaling is done to define the probability that a risk will occur. The scale can be based on word values such as Low, Medium, or High.
Percentage can also be assigned to these words, like 10% to low and 90% to high.
Impact- Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss.
However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Impact is expressed as a relative value. For example, low could be 10, medium could be 50, and high could be 100.
Risk level = Probability * Impact
Incorrect Answers:
B, D: These are used for calculating Annual loss expectancy (ALE) in quantitative risk assessment.
Formula is given as follows:
ALE= SLE * ARO

NEW QUESTION: 335
Which of the following is the BEST indicator of the effectiveness of IT risk management processes?
A. Time between when IT risk scenarios are identified and the enterprise's response.
B. Percentage of business users completing risk training.
C. Percentage of high-risk scenarios for which risk action plans have been developed.
D. Number of key risk indicators (KRIs) defined.
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 336
The BEST way to improve a risk register is to ensure the register:
A. is regularly audited.
B. contains the risk assessment completion date.
C. is updated based upon significant events.
D. documents possible countermeasures.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 337
An organization maintains independent departmental risk registers that are not automatically aggregated. Which of the following is the GREATEST concern?
A. Multiple risk treatment efforts may be initiated to treat a given risk.
B. Resources may be inefficiently allocated.
C. Management may be unable to accurately evaluate the risk profile.
D. The same risk factor may be identified in multiple areas.
Answer: (SHOW ANSWER)

NEW QUESTION: 338
Which of the following would BEST help to ensure that suspicious network activity is identified?
A. Analyzing server logs
B. Coordinating events with appropriate agencies
C. Analyzing intrusion detection system (IDS) logs
D. Using a third-party monitoring provider
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 339
You are the project manager of your enterprise. While performing risk management, you are given a task to identify where your enterprise stands in certain practice and also to suggest the priorities for improvements.
Which of the following models would you use to accomplish this task?
A. Capability maturity model
B. Decision tree model
C. Fishbone model
D. Simulation tree model
Answer: (SHOW ANSWER)
Section: Volume D
Explanation:
Capability maturity models are the models that are used by the enterprise to rate itself in terms of the least mature level (having nonexistent or unstructured processes) to the most mature (having adopted and optimized the use of good practices).
The levels within a capability maturity model are designed to allow an enterprise to identify descriptions of its current and possible future states. In general, the purpose is to:
* Identify, where enterprises are in relation to certain activities or practices.
* Suggest how to set priorities for improvements
Incorrect Answers:
D: There is no such model exists in risk management process.
B: Decision tree analysis is a risk analysis tool that can help the project manager in determining the best risk response. The tool can be used to measure probability, impact, and risk exposure

and how the selected risk response can affect the probability and/or impact of the selected risk event. It helps to form a balanced image of the risks and opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.
C: Fishbone diagrams or Ishikawa diagrams shows the relationships between the causes and effects of problems.

NEW QUESTION: 340
The PRIMARY objective of testing the effectiveness of a new control before implementation is to:
A. comply with the organization's policy.
B. ensure that risk is mitigated by the control.
C. measure efficiency of the control process.
D. confirm control alignment with business objectives.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 341
Malware has recently affected an organization, The MOST effective way to resolve this situation and define a comprehensive risk treatment plan would be to perform:
A. a root cause analysis.
B. a vulnerability assessment.
C. a gap analysis
D. an impact assessment.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 342
You work as a Project Manager for www.company.com Inc. You have to measure the probability, impact, and risk exposure. Then, you have to measure how the selected risk response can affect the probability and impact of the selected risk event. Which of the following tools will help you to accomplish the task?
A. Project network diagrams
B. Delphi technique
C. Decision tree analysis
D. Cause-and-effect diagrams
Answer: (SHOW ANSWER)
Section: Volume B
Explanation:
Decision tree analysis is a risk analysis tool that can help the project manager in determining the best risk response. The tool can be used to measure probability, impact, and risk exposure and how the selected risk response can affect the probability and/or impact of the selected risk event.

It helps to form a balanced image of the risks and opportunities connected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility.
Incorrect Answers:
A: Project network diagrams help the project manager and stakeholders visualize the flow of the project work, but they are not used as a part of risk response planning.
B: The Delphi technique can be used in risk identification, but generally is not used in risk response planning.
The Delphi technique uses rounds of anonymous surveys to identify risks.
D: Cause-and-effect diagrams are useful for identifying root causes and risk identification, but they are not the most effective ones for risk response planning.

NEW QUESTION: 343
Business areas within an organization have engaged various cloud service providers directly without assistance from the IT department. What should the risk practitioner do?
A. Engage with the business area managers to review controls applied.
B. Recommend a risk assessment be conducted.
C. Recommend the IT department remove access to the cloud services.
D. Escalate to the risk committee.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 344
An organization has four different projects competing for funding to reduce overall IT risk. Which project should management defer?

Project Name	Initial Risk Rating	Residual Risk Rating	Project Cost
Alpha	High	Medium	High
Bravo	High	Low	Medium
Charlie	High	High	High
Delta	High	Medium	Medium

A. Project Delta
B. Project Bravo
C. Project Alpha
D. Project Charlie
Answer: D (LEAVE A REPLY)

NEW QUESTION: 345
Which of the following would be a risk practitioner's BEST recommendation to help ensure cyber risk is assessed and reflected in the enterprise-level risk profile?
A. Conduct cyber risk awareness training tailored specifically for senior management

B. Implement a cyber risk program based on industry best practices
C. Manage cyber risk according to the organization's risk management framework
D. Define cyber roles and responsibilities across the organization
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 346
Which of the following will BEST quantify the risk associated with malicious users in an organization?
A. Threat risk assessment
B. Risk analysis
C. Vulnerability assessment
D. Business impact analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 347
Adrian is a project manager for a new project using a technology that has recently been released and there's relatively little information about the technology. Initial testing of the technology makes the use of it look promising, but there's still uncertainty as to the longevity and reliability of the technology. Adrian wants to consider the technology factors a risk for her project. Where should she document the risks associated with this technology so she can track the risk status and responses?
A. Project scope statement
B. Project charter
C. Risk low-level watch list
D. Risk register
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation:
A risk register is an inventory of risks and exposure associated with those risks. Risks are commonly found in project management practices, and provide information to identify, analyze, and manage risks. Typically a risk register contains:

* A description of the risk
* The impact should this event actually occur
* The probability of its occurrence
* Risk Score (the multiplication of Probability and Impact)
* A summary of the planned response should the event occur
* A summary of the mitigation (the actions taken in advance to reduce the probability and/or impact of the event)
* Ranking of risks by Risk Score so as to highlight the highest priority risks to all involved.
* It records the initial risks, the potential responses, and tracks the status of each identified risk in the project.

Incorrect Answers:

A: The project scope statement does document initially defined risks but it is not a place that will record risks responses and status of risks.

B: The project charter does not define risks.

C: The risk low-level watch list is for identified risks that have low impact and low probability in the project.

NEW QUESTION: 348

Which of the following assets are the examples of intangible assets of an enterprise?
Each correct answer represents a complete solution. Choose two.

A. Customer trust

B. Information

C. People

D. Infrastructure

Answer: A,B (LEAVE A REPLY)

Assets are the economic resources owned by business or company. Anything tangible or intangible that one possesses, usually considered as applicable to the payment of one's debts, is considered an asset. An asset can also be defined as a resource, process, product, computing infrastructure, and so forth that an organization has determined must be protected. Tangible asset: Tangible are those asset that has physical attributes and can be detected with the senses, e.g., people, infrastructure, and finances. Intangible asset: Intangible are those asset that has no physical attributes and cannot be detected with the senses, e.g., information, reputation and customer trust.

NEW QUESTION: 349

Which of the following is the STRONGEST indication an organization has ethics management issues?

A. Employees face sanctions for not signing the organization's acceptable use policy.

B. The organization has only two lines of defense.

C. Employees do not report IT risk issues for fear of consequences.

D. Internal IT auditors report to the chief information security officer (CISO).

Answer: C (LEAVE A REPLY)

NEW QUESTION: 350
You are the project manager of the QPS project. You and your project team have identified a pure risk. You along with the key stakeholders, decided to remove the pure risk from the project by changing the project plan altogether. What is a pure risk?
A. It is a risk event that only has a negative side and not any positive result.
B. It is a risk event that is created by the application of risk response.
C. It is a risk event that is generated due to errors or omission in the project work.
D. It is a risk event that cannot be avoided because of the order of the work.
E. Explanation:
A pure risk has only a negative effect on the project. Pure risks are activities that are dangerous to complete and manage such as construction, electrical work, or manufacturing. It is a class of risk
in which loss is the only probable result and there is no positive result.
Pure risk is associated to the events that are outside the risk-taker's control.
F. is incorrect. This in not valid definition of pure risk.
G. is incorrect. The risk event created by the application of risk response is called secondary risk.
Answer: (SHOW ANSWER)
is incorrect. A risk event that is generated due to errors or omission in the project work
is not necessarily pure risk.

NEW QUESTION: 351
Stephen is the project manager of the GBB project. He has worked with two subject matter experts and his project team to complete the risk assessment technique. There are approximately 47 risks that have a low probability and a low impact on the project. Which of the following answers best describes what Stephen should do with these risk events?
A. Because they are low probability and low impact, Stephen should accept the risks.
B. The low probability and low impact risks should be added to a watchlist for future monitoring.
C. Because they are low probability and low impact, the risks can be dismissed.
D. The low probability and low impact risks should be added to the risk register.
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The low probability and low impact risks should be added to a watchlist for future monitoring.
Incorrect Answers:
A: The risk response for these events may be to accept them, but the best answer is to first add them to a watchlist.
C: Risks are not dismissed; they are at least added to a watchlist for monitoring.

D: While the risks may eventually be added to the register, the best answer is to first add them to the watchlist for monitoring.

NEW QUESTION: 352
Which of the following come under the phases of risk identification and evaluation?
Each correct answer represents a complete solution. Choose three.
A. Maintain a risk profile
B. Collecting data
C. Analyzing risk
D. Applying controls
Answer: A,B,C (LEAVE A REPLY)
Section: Volume D
Explanation:
Risk identification is the process of determining which risks may affect the project. It also documents risks' characteristics.
Following are high-level phases that are involved in risk identification and evaluation:
* Collecting data- Involves collecting data on the business environment, types of events, risk categories, risk scenarios, etc., to identify relevant data to enable effective risk identification, analysis and reporting.
* Analyzing risk- Involves analyzing risk to develop useful information which is used while taking risk- decisions. Risk-decisions take into account the business relevance of risk factors.
* Maintain a risk profile- Requires maintaining an up-to-date and complete inventory of known threats and their attributes (e.g., expected likelihood, potential impact, and disposition), IT resources, capabilities, and controls as understood in the context of business products, services and processes to effectively monitor risk over time.
Incorrect Answers:
D: It comes under risk management process, and not in risk identification and evaluation process.

NEW QUESTION: 353
Which of the following is the MOST important component of effective security incident response?
A. Identification of attack sources
B. A documented communications plan
C. Early detection of breaches
D. Network time protocol synchronization
Answer: (SHOW ANSWER)

NEW QUESTION: 354
An IT department has organized training sessions to improve user awareness of organizational information security policies. Which of the following is the BEST key performance indicator (KPI) to reflect effectiveness of the training?
A. Percentage of staff members who complete the training with a passing score

B. Percentage of attendees versus total staff
C. Number of training sessions completed
D. Percentage of staff members who attend the training with positive feedback
Answer: A (LEAVE A REPLY)

NEW QUESTION: 355
An unauthorized individual has socially engineered entry into an organization's secured physical premises.
Which of the following is the BEST way to prevent future occurrences?
A. Install security cameras.
B. Conduct security awareness training.
C. Employ security guards.
D. Require security access badges.
Answer: (SHOW ANSWER)

NEW QUESTION: 356
Which of the following should be included in a risk assessment report to BEST facilitate senior management's understanding of the results?
A. The possible impact of internal and external risk factors on the assessment results
B. A risk heat map with a summary of risk identified and assessed
C. Tools and techniques used by risk owners to perform the assessments
D. Benchmarking parameters likely to affect the results
Answer: B (LEAVE A REPLY)

NEW QUESTION: 357
A risk assessment has identified that an organization may not be in compliance with industry regulations. The BEST course of action would be to:
A. collaborate with management to meet compliance requirements
B. conduct a gap analysis against compliance criteria
C. identify necessary controls to ensure compliance
D. modify internal assurance activities to include control validation
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 358
What is the most important benefit of classifying information assets?
A. Linking security requirements to business objectives
B. Allotting risk ownership
C. Defining access rights
D. Identifying controls that should be applied

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

All of the options are directly or indirectly are the advantages of classifying information assets, but the most important benefit amongst them is that appropriate controls can be identified.

Incorrect Answers:

A, B, C: These all are less significant than identifying controls.

NEW QUESTION: 359

Which of the following are the MOST important risk components that must be communicated among all the stakeholders?

Each correct answer represents a part of the solution. Choose three.

A. Various risk response used in the project

B. Expectations from risk management

C. Current risk management capability

D. Status of risk with regard to IT risk

Answer: B,C,D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

The broad array of information and the major types of IT risk information that should be communicated are as follows:

- Expectations from risk management: They include risk strategy, policies, procedures, awareness training, uninterrupted reinforcement of principles, etc. This essential communication drives all subsequent efforts on risk management and sets the overall expectations from risk management.
- Current risk management capability: This allows monitoring of the status of the risk management engine in the enterprise. It is a key indicator for effective risk management and has predictive value for how well the enterprise is managing risk and reducing exposure.
- Status with regard to IT risk: This describes the actual status with regard to IT risk including information of risk profile of the enterprise, Key risk indicators (KRIs) to support management reporting on risk, event-loss data, root cause of loss events and options to mitigate risk.

Incorrect Answers:

A: Risk response is only communicated to some of the stakeholders not all, as it is irrelevant for them. It is not communicated to the stakeholders of the project like project sponsors, etc.

NEW QUESTION: 360

John is the project manager of the NHQ Project for his company. His project has 75 stakeholders, some of which are external to the organization. John needs to make certain that he communicates about risk in the most appropriate method for the external stakeholders. Which

project management plan will be the best guide for John to communicate to the external stakeholders?

A. Risk Response Plan

B. Communications Management Plan

C. Project Management Plan

D. Risk Management Plan

E. Explanation:

The Communications Management Plan will direct John on the information to be communicated, when to communicate, and how to communicate with external stakeholders. The Communications Management Plan aims to define the communication necessities for the project and how the information will be circulated. The Communications Management Plan sets the communication structure for the project. This structure provides guidance for communication throughout the project's life and is updated as communication needs change. The Communication Managements Plan identifies and defines the roles of persons concerned with the project. It includes a matrix known as the communication matrix to map the communication requirements of the project.

Answer: B (LEAVE A REPLY)

is incorrect. The Risk Management Plan defines how risks will be identified, analyzed, responded to, and controlled throughout the project. Answer:A is incorrect. The Risk Response Plan identifies how risks will be responded to. Answer:C is incorrect. The Project Management Plan is the parent of all subsidiary management plans and it is not the most accurate choice for this

NEW QUESTION: 361

Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?

A. Risk heat maps

B. Key performance indicators (KPIs)

C. Periodic penetration testing

D. Internal audit findings

Answer: C (LEAVE A REPLY)

NEW QUESTION: 362

Which of the following is MOST important for a risk practitioner to consider when determining the control requirements for data privacy arising from emerging technologies?
A. Laws and regulations
B. internal audit recommendations
C. Policies and procedures
D. Standards and frameworks
Answer: A (LEAVE A REPLY)

NEW QUESTION: 363
What are the MOST essential attributes of an effective Key control indicator (KCI)?
A. Robustness and resilience
B. Optimal cost and benefit
C. Flexibility and adaptability
D. Measurability and consistency
Answer: D (LEAVE A REPLY)

NEW QUESTION: 364
The MOST essential content to include in an IT risk awareness program is how to:
A. populate risk register entries and build a risk profile for management reporting.
B. prioritize IT-related actions by considering risk appetite and risk tolerance.
C. define the IT risk framework for the organization. .
D. comply with the organization's IT risk and information security policies.
Answer: (SHOW ANSWER)

NEW QUESTION: 365
Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?
A. Information security director
B. Internal audit director
C. Chief information officer
D. Chief financial officer
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 366
The annualized loss expectancy (ALE) method of risk analysis:
A. can be used m a cost-benefit analysts
B. helps in calculating the expected cost of controls
C. uses qualitative risk rankings such as low. medium and high.
D. can be used to determine the indirect business impact.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 367
Which of the following is MOST effective in continuous risk management process improvement?
A. Change management
B. Awareness training
C. Policy updates
D. Periodic assessments
Answer: (SHOW ANSWER)

NEW QUESTION: 368
Which of the following processes is described in the statement below?
"It is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions."
A. Risk governance
B. IRGC
C. Risk response planning
D. Risk communication
Answer: D (LEAVE A REPLY)
Section: Volume B
Explanation:
Risk communication is the process of exchanging information and views about risks among stakeholders, such as groups, individuals, and institutions. Risk communication is mostly concerned with the nature of risk or expressing concerns, views, or reactions to risk managers or institutional bodies for risk management. The key plan to consider and communicate risk is to categorize and impose priorities, and acquire suitable measures to reduce risks. It is important throughout any crisis to put across multifaceted information in a simple and clear manner. Risk communication helps in switching or allocating the information concerning risk among the decision-maker and the stakeholders. Risk communication can be explained more clearly with the help of the following definitions:
* It defines the issue of what a group does, not just what it says.
* It must take into account the valuable element in user's perceptions of risk.
* It will be more valuable if it is thought of as conversation, not instruction.
Risk communication is a fundamental and continuing element of the risk analysis exercise, and the involvement of the stakeholder group is from the beginning. It makes the stakeholders conscious of the process at each phase of the risk assessment. It helps to guarantee that the restrictions, outcomes, consequence, logic, and risk assessment are undoubtedly understood by all the stakeholders.
Incorrect Answers:
A: Risk governance is a systemic approach to decision making processes associated to natural and technological risks. It is based on the principles of cooperation, participation, mitigation and sustainability, and is adopted to achieve more effective risk management. It seeks to reduce risk

exposure and vulnerability by filling gaps in risk policy, in order to avoid or reduce human and economic costs caused by disasters.
Risk governance is a continuous life cycle that requires regular reporting and ongoing review. The risk governance function must oversee the operations of the risk management team.
B: The International Risk Governance Council (IRGC) is a self-governing organization whose principle is to facilitate the understanding and managing the rising overall risks that have impacts on the economy and society, human health and safety, the environment at large. IRGC's effort is to build and develop concepts of risk governance, predict main risk issues and present risk governance policy recommendations for the chief decision makers. IRGC mainly emphasizes on rising, universal risks for which governance deficits exist.
Its goal is to present recommendations for how policy makers can correct them. IRGC models at constructing strong, integrative inter-disciplinary governance models for up-coming and existing risks.
C: Risk response is a process of deciding what measures should be taken to reduce threats and take advantage of the opportunities discovered during the risk analysis processes. This process also includes assigning departments or individual staff members the responsibility of carrying out the risk response plans and these folks are known as risk owners.
The prioritization of the risk responses and development of the risk response plan is based on following parameters:
* Cost of the response to reduce risk within tolerance levels
* Importance of the risk
* Capability to implement the response
* Effectiveness and efficiency of the response
Risk prioritization strategy is used to create a risk response plan and implementation schedule because all risk cannot be addressed at the same time. It may take considerable investment of time and resources to address all the risk identified in the risk analysis process. Risk with a greater likelihood and impact on the enterprise will prioritized above other risk that is considered less likely or lay less impact.

NEW QUESTION: 369
Which of the following is the BEST way to quantify the likelihood of risk materialization?
A. Business impact analysis (BIA)
B. Compliance assessments
C. Threat and vulnerability assessment
D. Balanced scorecard
Answer: A (LEAVE A REPLY)

NEW QUESTION: 370
Ben is the project manager of the CMH Project for his organization. He has identified a risk that has a low probability of happening, but the impact of the risk event could save the project and the organization with a significant amount of capital. Ben assigns Laura to the risk event and instructs

her to research the time, cost, and method to improve the probability of the positive risk event. Ben then communicates the risk event and response to management. What risk response has been used here?

A. Transference

B. Enhance

C. Exploit

D. Sharing

Answer: B (LEAVE A REPLY)

Section: Volume B

Explanation:

Enhance is a risk response to improve the conditions to ensure the risk event occurs. Risk enhancement raises the probability of an opportunity to take place by focusing on the trigger conditions of the opportunity and optimizing the chances. Identifying and maximizing input drivers of these positive-impact risks may raise the probability of their occurrence.

Incorrect Answers:

A: Transference is a strategy to mitigate negative risks or threats. In this strategy, consequences and the ownership of a risk is transferred to a third party. This strategy does not eliminate the risk but transfers responsibility of managing the risk to another party. Insurance is an example of transference.

C: Exploit response is one of the strategies to negate risks or threats that appear in a project. This strategy may be selected for risks with positive impacts where the organization wishes to ensure that the opportunity is realized. Exploiting a risk event provides opportunities for positive impact on a project. Assigning more talented resources to the project to reduce the time to completion is an example of exploit response.

D: Sharing happens through partnerships, joint ventures, and teaming agreements. Sharing response is where two or more entities share a positive risk. Teaming agreements are good example of sharing the reward that comes from the risk of the opportunity.

NEW QUESTION: 371

An effective control environment is BEST indicated by controls that:

A. minimize senior management's risk tolerance

B. manage risk within the organization's risk appetite

C. are cost-effective to implement

D. reduce the thresholds of key risk indicators (KRIs)

Answer: D (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 372

The BEST key performance indicator (KPI) to measure the effectiveness of a vendor risk management program is the percentage of:

A. vendor contracts reviewed in the past year.

B. vendors that have reported control-related incidents.
C. vendors providing risk assessments on time.
D. vendor risk mitigation action items completed on time.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 373
During a routine check, a system administrator identifies unusual activity indicating an intruder within a firewall.
Which of the following controls has MOST likely been compromised?
A. Authentication
B. Identification
C. Data validation
D. Data integrity
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation/Reference: https://resources.infosecinstitute.com/network-design-firewall-idsips/#gref

NEW QUESTION: 374
The compensating control that MOST effectively addresses the risk associated with piggybacking into a restricted area without a dead-man door is:
A. using two-factor authentication
B. using biometric door locks
C. requiring employees to wear ID badges
D. security awareness training
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 375
You are the program manager for your organization and you are working with Alice, a project manager in her program. Alice calls you and insists you to add a change to program scope. You agree for that the change. What must Alice do to move forward with her change request?
A. Add the change to the program scope herself, as she is a project manager
B. Create a change request charter justifying the change request
C. Document the change request in a change request form.
D. Add the change request to the scope and complete integrated change control
Answer: C (LEAVE A REPLY)
Change requests must be documented to be considered. Alice should create a change request form and follow the procedures of the change control system.

NEW QUESTION: 376

The GREATEST benefit of including low-probability, high-impact events in a risk assessment is the ability to:
A. perform an aggregated cost-benefit analysis
B. identify root causes for relevant events
C. develop a comprehensive risk mitigation strategy
D. develop understandable and realistic risk scenarios
Answer: A (LEAVE A REPLY)

NEW QUESTION: 377
You are working with a vendor on your project. A stakeholder has requested a change for the project, which will add value to the project deliverables. The vendor that you're working with on the project will be affected by the change. What system can help you introduce and execute the stakeholder change request with the vendor?
A. Contract change control system
B. Scope change control system
C. Cost change control system
D. Schedule change control system
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The contract change control system is part of the project's change control system. It addresses changes with the vendor that may affect the project contract. Change control system, a part of the configuration management system, is a collection of formal documented procedures that define how project deliverables and documentation will be controlled, changed, and approved.
Incorrect Answers:
B: The scope may change because of the stakeholder change request.
Vendor's relationship to the project, hence this choice is not the best answer.
C: The cost change control system manages changes to costs in the project.
D: There is no indication that the change could affect the project schedule.

NEW QUESTION: 378

Which of the following BEST measures the operational effectiveness of risk management capabilities?

A. Capability maturity models (CMMs)

B. Metric thresholds

C. Key risk indicators (KRIs)

D. Key performance indicators (KPIs)

E. Explanation:

Key performance indicators (KPIs) provide insights into the operational effectiveness of the concept or capability that they monitor. Key Performance Indicators is a set of measures that a company or industry uses to measure and/or compare performance in terms of meeting their strategic and operational goals. KPIs vary with company to company, depending on their priorities or performance criteria. A company must establish its strategic and operational goals and then choose their KPIs which can best reflect those goals. For example, if a software company's goal is to have the fastest growth in its industry, its main performance indicator may be the measure of its annualrevenue growth.

Answer: D,E (LEAVE A REPLY)

is incorrect. Key risk indicators (KRIs) only provide insights into potential risks that may exist or be realized within a concept or capability that they monitor. Key Risk Indicators are the prime monitoring indicators of the enterprise. KRIs are highly relevant and possess a high probability of predicting or indicating important risk. KRIs help in avoiding excessively large number of risk indicators to manage and report that a large enterprise may have. Answer: A is incorrect. Capability maturity models (CMMs) assess the maturity of a concept or capability and do not provide insights into operational effectiveness. Answer: B is incorrect. Metric thresholds are decision or action points that are enacted when a KPI or KRI reports a specific value or set of values. It odes not provide any insights into operational effectiveness.

NEW QUESTION: 379

Which of the following is MOST effective against external threats to an organizations confidential information?

A. Intrusion detection system

B. Data integrity checking

C. Single sign-on

D. Strong authentication

Answer: D (LEAVE A REPLY)

NEW QUESTION: 380

During qualitative risk analysis you want to define the risk urgency assessment. All of the following are indicators of risk priority except for which one?

A. Warning signs

B. Symptoms

C. Risk rating

D. Cost of the project
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The cost of the project is not an indicator of risk urgency. The affect of the risk on the overall cost of the project may be considered, but it is not the best answer.
Incorrect Answers:
A: Warning signs are an indicator of the risk urgency.
B: Symptoms are an indicator of the risk urgency.
C: The risk rating can be an indicator of the risk urgency.

NEW QUESTION: 381
Senior management has asked a risk practitioner to develop technical risk scenarios related to a recently developed enterprise resource planning (ERP) system. These scenarios will be owned by the system manager. Which of the following would be the BEST method to use when developing the scenarios?
A. Bottom-up approach
B. Cause-and-effect diagram
C. Delphi technique
D. Top-down approach
Answer: B (LEAVE A REPLY)

NEW QUESTION: 382
A maturity model will BEST indicate:
A. effectiveness and efficiency.
B. confidentiality and integrity.
C. certification and accreditation.
D. availability and reliability.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 383
Mapping open risk issues to an enterprise risk heat map BEST facilitates:
A. risk identification.
B. risk response.
C. control monitoring.
D. risk ownership.
Answer: (SHOW ANSWER)

NEW QUESTION: 384

You are the project manager of the NGQQ Project for your company. To help you communicate project status to your stakeholders, you are going to create a stakeholder register. All of the following information should be included in the stakeholder register except for which one?
A. Stakeholder management strategy
B. Assessment information of the stakeholders' major requirements, expectations, and potential influence
C. Identification information for each stakeholder
D. Stakeholder classification of their role in the project
Answer: A (LEAVE A REPLY)
Section: Volume C
Explanation:
The stakeholder management strategy is generally not included in the stakeholder registry because it may contain sensitive information that should not be shared with project team members or certain other individuals that could see the stakeholder register. The stakeholder register is a project management document that contains a list of the stakeholders associated with the project. It assesses how they are involved in the project and identifies what role they play in the organization. The information in this document can be very perceptive and is meant for limited exchange only. It also contains relevant information about the stakeholders, such as their requirements, expectations, and influence on the project.
Incorrect Answers:
B, C, D: Stakeholder identification, Assessment information, and Stakeholder classification should be included in the stakeholder register.

NEW QUESTION: 385
Which of the following would BEST help identify the owner for each risk scenario in a risk register?
A. Allocating responsibility for risk factors equally to asset owners.
B. Determining resource dependency of assets.
C. Mapping identified risk factors to specific business processes.
D. Determining which departments contribute most to risk.
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 386
Which of the following is the MOST important objective of an enterprise risk management (ERM) program?
A. To optimize costs of managing risk scenarios in the organization
B. To provide a bottom-up view of the most significant risk scenarios
C. To create a comprehensive view of critical risk to the organization
D. To create a complete repository of risk to the organization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 387
Which of the following is MOST helpful to ensure effective security controls for a cloud service provider?
A. A third-party security assessment report
B. Service level agreement monitoring
C. Internal audit reports from the vendor
D. A control self-assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 388
Which of the following would be MOST beneficial as a key risk indicator (KRI)?
A. Negative security return on investment (ROI)
B. Current capital allocation reserves
C. Project cost variances
D. Annualized loss projections
Answer: (SHOW ANSWER)

NEW QUESTION: 389
Which of the following would provide executive management with the BEST information to make risk decisions as a result of a risk assessment?
A. A quantitative presentation of risk assessment results
B. A qualitative presentation of risk assessment results
C. A companion of risk assessment results to the desired state
D. An assessment of organizational maturity levels and readiness
Answer: B (LEAVE A REPLY)

NEW QUESTION: 390
Which of the following come under the management class of controls?
Each correct answer represents a complete solution. Choose all that apply.
A. Risk assessment control
B. Audit and accountability control
C. Program management control
D. Identification and authentication control
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The Management class of controls includes five families. These families include over 40 individual controls.
Following is a list of each of the families in the Management class:

Certification, Accreditation, and Security Assessment (CA): This family of controls addresses steps to
- implement a security and assessment program. It includes controls to ensure only authorized systems are allowed on a network. It includes details on important security concepts, such as continuous monitoring and a plan of action and milestones.

Planning (PL): The PL family focuses on security plans for systems. It also covers Rules of Behaviour
- for users. Rules of Behaviour are also called an acceptable use policy.

Risk Assessment (RA): This family of controls provides details on risk assessments and vulnerability
- scanning.

System and Services Acquisition (SA): The SA family includes any controls related to the purchase of
- products and services. It also includes controls related to software usage and user installed software.

Program Management (PM): This family is driven by the Federal Information Security Management Act
- (FISMA). It provides controls to ensure compliance with FISMA. These controls complement other controls. They don't replace them.

Incorrect Answers:
B, D: Identification and authentication, and audit and accountability control are technical class of controls.

NEW QUESTION: 391
The MAIN purpose of reviewing a control after implementation is to validate that the control:
A. operates efficiently.
B. is being monitored.
C. operates as intended.
D. meets regulatory requirements.
Answer: (SHOW ANSWER)

NEW QUESTION: 392
Which of the following is the MOST common concern associated with outsourcing to a service provider?
A. Combining incompatible duties
B. Unauthorized data usage
C. Denial of service attacks
D. Lack of technical expertise
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 393
You have been assigned as the Project Manager for a new project that involves building of a new roadway between the city airport to a designated point within the city. However, you notice that the transportation permit issuing authority is taking longer than the planned time to issue the permit to begin construction. What would you classify this as?
A. Project Risk
B. Status Update
C. Risk Update
D. Project Issue
E. Explanation:
This is a project issue. It is easy to confuse this as a project risk; however, a project risk is always in the future. In this case, the delay by the permitting agency has already happened; hence this is a project issue. The possible impact of this delay on the project cost, schedule, or performance can be classified as a project risk.
F. is incorrect. It is easy to confuse this as a project risk; however, a project risk is always in the future. In this case, the delay by the permitting agency has already happened; hence this is a project issue.
Answer: D,E,F (LEAVE A REPLY)
and B are incorrect as they are extraneous choices and are not applicable.

NEW QUESTION: 394
Numerous media reports indicate a recently discovered technical vulnerability is being actively exploited. Which of the following would be the BEST response to this scenario?
A. Conduct a control serf-assessment.
B. Assess the vulnerability management process.
C. Conduct a vulnerability assessment.
D. Reassess the inherent risk of the target.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 395

You work as a project manager for BlueWell Inc. Management has asked you to work with the key project stakeholder to analyze the risk events you have identified in the project. They would like you to analyze the project risks with a goal of improving the project's performance as a whole. What approach can you use to achieve this goal of improving the project's performance through risk analysis with your project stakeholders?

A. Involve subject matter experts in the risk analysis activities

B. Involve the stakeholders for risk identification only in the phases where the project directly affects them

C. Use qualitative risk analysis to quickly assess the probability and impact of risk events

D. Focus on the high-priority risks through qualitative risk analysis

Answer: (SHOW ANSWER)

Section: Volume A

Explanation:

By focusing on the high-priority of risk events through qualitative risk analysis you can improve the project's performance.

Qualitative analysis is the definition of risk factors in terms of high/medium/low or a numeric scale (1 to 10).

Hence it determines the nature of risk on a relative scale.

Some of the qualitative methods of risk analysis are:

* Scenario analysis- This is a forward-looking process that can reflect risk for a given point in time.

* Risk Control Self -assessment (RCSA) - RCSA is used by enterprises (like banks) for the identification and evaluation of operational risk exposure. It is a logical first step and assumes that business owners and managers are closest to the issues and have the most expertise as to the source of the risk. RCSA is a constructive process in compelling business owners to contemplate, and then explain, the issues at hand with the added benefit of increasing their accountability.

Incorrect Answers:

A: Subject matter experts can help the qualitative risk assessment, but by focusing on high-priority risks the project's performance can improve by addressing these risk events.

B: Stakeholders should be involved throughout the project as situations within the project demand their input to risk identification and analysis.

C: Qualitative analysis does use a fast approach of analyzing project risks, but it's not the best answer for this

NEW QUESTION: 396

Where are all risks and risk responses documented as the project progresses?

A. Risk management plan

B. Project management plan

C. Risk response plan

D. Risk register

Answer: D (LEAVE A REPLY)

Section: Volume A
Explanation:
All risks, their responses, and other characteristics are documented in the risk register. As the project progresses and the conditions of the risk events change, the risk register should be updated to reflect the risk conditions.
Incorrect Answers:
A: The risk management plan addresses the project management's approach to risk management, risk identification, analysis, response, and control.
B: The project management plan is the overarching plan for the project, not the specifics of the risk responses and risk identification.
C: The risk response plan only addresses the planned risk responses for the identified risk events in the risk register.

NEW QUESTION: 397
It is MOST appropriate for changes to be promoted to production after they are;
A. tested by business owners.
B. approved by the business owner.
C. initiated by business users.
D. communicated to business management
Answer: (SHOW ANSWER)

NEW QUESTION: 398
Which of the following provides the MOST important information to facilitate a risk response decision?
A. Audit findings
B. Risk appetite
C. Industry best practices
D. Key risk indicators
Answer: B (LEAVE A REPLY)

NEW QUESTION: 399
Which of the following is the BEST indication that an organization is following a mature risk management process?
A. Executive management receives periodic risk awareness training.
B. Attributes of each risk scenario have been documented within the risk register.
C. The risk register is frequently utilized for decision-making.
D. A dashboard has been developed for senior management to provide real-time risk values.
Answer: D (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 400

What are the various outputs of risk response?

A. Risk Priority Number

B. Residual risk

C. Risk register updates

D. Project management plan and Project document updates

E. Risk-related contract decisions

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

The outputs of the risk response planning process are:

Risk Register Updates: The risk register is written in detail so that it can be related to the priority ranking and the planned response.

Risk Related Contract Decisions: Risk related contract decisions are the decisions to transmit risk, such as services, agreements for insurance, and other items as required. It provides a means for sharing risks.

Project Management Plan Updates: Some of the elements of the project management plan updates are:

- Schedule management plan
- Cost management plan
- Quality management plan
- Procurement management plan
- Human resource management plan
- Work breakdown structure
- Schedule baseline
- Cost performance baseline

Project Document Updates: Some of the project documents that can be updated includes:

- Assumption log updates
- Technical documentation updates

Incorrect Answers:

A: Risk priority number is not an output for risk response but instead it is done before applying response.

Hence it act as one of the inputs of risk response and is not the output of it.

B: Residual risk is not an output of risk response. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk. As, Risk = Threat Vulnerability and Total risk = Threat Vulnerability Asset Value Residual risk can be calculated with the following formula:

Residual Risk = Total Risk - Controls

Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, transferred, mitigated or accepted. They also decide what controls to implement. Any loss due to their decisions falls on their sides.
Residual risk assessments are conducted after mitigation to determine the impact of the risk on the enterprise. For risk assessment, the effect and frequency is reassessed and the impact is recalculated.

NEW QUESTION: 401
You are the project manager of your enterprise. While performing risk management, you are given a task to identify where your enterprise stand in certain practice and also to suggest the priorities for improvements. Which of the following models would you use to accomplish this task?
A. Capability maturity model
B. Decision tree model
C. Fishbone model
D. Simulation tree model
E. Explanation:
Capability maturity models are the models that are used by the enterprise to rate itself in terms of the least mature level (having nonexistent or unstructured processes) to the most mature (having adopted and optimized the use of good practices). The levels within a capability maturity model are designed to allow an enterprise to identify descriptions of its current and possible future states. In general, the purpose is to: Identify, where enterprises are in relation to certain activities or practices. Suggest how to set priorities for improvements
Answer: (SHOW ANSWER)
is incorrect. There is no such model exists in risk management process. Answer:B is incorrect. Decision tree analysis is a risk analysis tool that can help the project manager in determining the best risk response. The tool can be used to measure probability, impact, and risk exposure and how the selected risk response can affect the probability and/or impact of the selected risk event. It helps to form a balanced image of the risks andopportunitiesconnected with each possible course of action. This makes them mostly useful for choosing between different strategies, projects, or investment opportunities particularly when the resources are limited. A decision tree is a decision support tool that uses a tree-like graph or model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. Answer:C is incorrect. Fishbone diagrams or Ishikawa diagrams shows the relationships between the causes and effects of problems.

NEW QUESTION: 402
Which of following is NOT used for measurement of Critical Success Factors of the project?
A. Productivity
B. Quality
C. Quantity
D. Customer service

Answer: C (LEAVE A REPLY)
Answer A, B, and D are incorrect. Productivity, quality and customer service are used for evaluating critical service factor of any particular project.

NEW QUESTION: 403
An organization is implementing encryption for data at rest to reduce the risk associated with unauthorized access. Which of the following MUST be considered to assess the residual risk?
A. Data retention requirements
B. Data destruction requirements
C. Cloud storage architecture
D. Key management
Answer: (SHOW ANSWER)

NEW QUESTION: 404
Which of the following is the MOST important objective of embedding risk management practices into the initiation phase of the project management life cycle?
A. To assess inherent risk
B. To deliver projects on time and on budget
C. To assess risk throughout the project
D. To include project risk in the enterprise-wide IT risk profit.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 405
Which of the following is MOST important when developing risk scenarios?
A. Reviewing business impact analysis (BIA)
B. Obtaining input from key stakeholders
C. Collaborating with IT audit
D. Conducting vulnerability assessments
Answer: B (LEAVE A REPLY)

NEW QUESTION: 406
Which of the following is the MOST important consideration when identifying stakeholders to review risk scenarios developed by a risk analyst? The reviewers are:
A. authorized to select risk mitigation options.
B. independent from the business operations.
C. accountable for the affected processes.
D. members of senior management.
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 407
A risk assessment has identified increased losses associated with an IT risk scenario. It is MOST important for the risk practitioner to:
A. implement additional controls.
B. develop new risk scenarios.
C. update the risk rating.
D. reevaluate inherent risk.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 408
Which of the following is MOST important to have in place to ensure the effectiveness of risk and security metrics reporting?
A. Regularly scheduled audits
B. Organizational reporting process
C. Incident reporting procedures
D. Incident management policy
Answer: A (LEAVE A REPLY)

NEW QUESTION: 409
Which of the following would require updates to an organization's IT risk register?
A. Completion of the latest internal audit
B. Changes to the team responsible for maintaining the register
C. Discovery of an ineffectively designed key IT control
D. Management review of key risk indicators (KRIs)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 410
You and your project team are identifying the risks that may exist within your project. Some of the risks are small risks that won't affect your project much if they happen. What should you do with these identified risk events?
A. These risks can be dismissed.
B. These risks can be accepted.

C. These risks can be added to a low priority risk watch list.
D. All risks must have a valid, documented risk response.
Answer: C (LEAVE A REPLY)
Section: Volume C
Explanation
Explanation:
Low-impact, low-probability risks can be added to the low priority risk watch list.
Incorrect Answers:
A: These risks are not dismissed; they are still documented on the low priority risk watch list.
B: While these risks may be accepted, they should be documented on the low priority risk watch list. This list will be periodically reviewed and the status of the risks may change.
D: Not every risk demands a risk response, so this choice is incorrect.

NEW QUESTION: 411
Which of the following is the process of numerically analyzing the effects of identified risks on the overall enterprise's objectives?
A. Identifying Risks
B. Quantitative Risk Assessment
C. Qualitative Risk Assessment
D. Monitoring and Controlling Risks
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A quantitative risk assessment quantifies risk in terms of numbers such as dollar values. This involves gathering data and then entering it into standard formulas. The results can help in identifying the priority of risks. These results are also used to determine the effectiveness of controls. Some of the terms associated with quantitative risk assessments are:
Single loss expectancy (SLE)-It refers to the total loss expected from a single incident. This incident
- can occur when vulnerability is being exploited by threat. The loss is expressed as a dollar value such as $1,000. It includes the value of data, software, and hardware.
SLE = Asset value * Exposure factor
Annual rate of occurrence (ARO)-It refers to the number of times expected for an incident to occur in a
- year. If an incident occurred twice a month in the past year, the ARO is 24. Assuming nothing changes, it is likely that it will occur 24 times next year.
Annual loss expectancy (ALE)-It is the expected loss for a year. ALE is calculated by multiplying SLE
- with ARO. Because SLE is a given in a dollar value, ALE is also given in a dollar value. For example, if the SLE is $1,000 and the ARO is 24, the ALE is $24,000. ALE = SLE * ARO

Safeguard value-This is the cost of a control. Controls are used to mitigate risk. For example, antivirus
- software of an average cost of $50 for each computer. If there are 50 computers, the safeguard value is
$2,500.

Incorrect Answers:

A: The first thing we must do in risk management is to identify the areas of the project where the risks can occur. This is termed as risk identification. Listing all the possible risks is proved to be very productive for the enterprise as we can cure them before it can occur. In risk identification both threats and opportunities are considered, as both carry some level of risk with them.

C: Unlike the quantitative risk assessment, qualitative risk assessment does not assign dollar values.

Rather, it determines risk's level based on the probability and impact of a risk. These values are determined by gathering the opinions of experts.

Probability- establishing the likelihood of occurrence and reoccurrence of specific risks, independently,
- and combined. The risk occurs when a threat exploits vulnerability. Scaling is done to define the probability that a risk will occur. The scale can be based on word values such as Low, Medium, or High.

Percentage can also be assigned to these words, like 10% to low and 90% to high.

Impact- Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss.
- However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Impact is expressed as a relative value. For example, low could be 10, medium could be 50, and high could be 100.

Risk level = Probability*Impact

D: This is the process of implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness through the project.

NEW QUESTION: 412

How residual risk can be determined?

A. By determining remaining vulnerabilities after countermeasures are in place.

B. By transferring all risks.

C. By threat analysis

D. By risk assessment

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

All risks are determined by risk assessment, regardless whether risks are residual or not.

Incorrect Answers:

A: Determining remaining vulnerabilities after countermeasures are in place says nothing about threats, therefore risk cannot be determined.
B: Transferring all the risks in not relevant to determining residual risk. It is one of the method of risk management.
C: Risk cannot be determined by threat analysis alone, regardless whether it is residual or not.

NEW QUESTION: 413
Marie has identified a risk event in her project that needs a mitigation response. Her response actually creates a new risk event that must now be analyzed and planned for. What term is given to this newly created risk event?
A. Residual risk
B. Secondary risk
C. Infinitive risk
D. Populated risk
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Secondary risks are the risks that come about as a result of implementing a risk response. This new risk event must be recorded, analyzed, and planned for management.
Incorrect Answers:
A: A residual risk event is similar to a secondary risk, but is often small in probability and impact, so it may just be accepted.
C: Infinitive risk is not a valid project management term.
D: Populated risk event is not a valid project management term.

NEW QUESTION: 414
Which of the following is the MAIN reason to continuously monitor IT-related risk?
A. To update the risk register to reflect changes in levels of identified and new IT-related risk
B. To ensure risk levels are within acceptable limits of the organization's risk appetite and risk tolerance
C. To help identify root causes of incidents and recommend suitable long-term solutions
D. To redefine the risk appetite and risk tolerance levels based on changes in risk factors
Answer: B (LEAVE A REPLY)

NEW QUESTION: 415
Jeff works as a Project Manager for www.company.com Inc. He and his team members are involved in the identify risk process. Which of the following tools & techniques will Jeff use in the identify risk process?
Each correct answer represents a complete solution. (Choose three.)
A. Information gathering technique
B. Documentation reviews

C. Checklist analysis
D. Risk categorization
Answer: (SHOW ANSWER)
Section: Volume B
Explanation
Explanation:
The various tools & techniques used in the identify risk process are as follows:
* Documentation reviews
* Information gathering technique
* Checklist analysis
* Assumption analysis
* Diagramming techniques
* SWOT analysis
* Expert judgment

NEW QUESTION: 416
Capability maturity models are the models that are used by the enterprise to rate itself in terms of the least mature level to the most mature level. Which of the following capability maturity levels shows that the enterprise does not recognize the need to consider the risk management or the business impact from IT risk?
A. Level 2
B. Level 0
C. Level 3
D. Level 1
Answer: B (LEAVE A REPLY)
Section: Volume B
Explanation:
0 nonexistent: An enterprise's risk management capability maturity level is 0 when:
* The enterprise does not recognize the need to consider the risk management or the business impact from IT risk.
* Decisions involving risk lack credible information.
* Awareness of external requirements for risk management and integration with enterprise risk management (ERM) do not exists.
Incorrect Answers:
A, C, D: These all are higher levels of capability maturity model and in this enterprise is mature enough to recognize the importance of risk management.

NEW QUESTION: 417
Controls should be defined during the design phase of system development because:
A. structured programming techniques require that controls be designed before coding begins.
B. it is more cost-effective to determine controls in the early design phase.

C. technical specifications are defined during this phase.
D. structured analysis techniques exclude identification of controls.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 418
You are the project manager in your enterprise. You have identified risk that is noticeable failure threatening the success of certain goals of your enterprise. In which of the following levels do this identified risk exists?
A. Moderate risk
B. High risk
C. Extremely high risk
D. Low risk
Answer: A (LEAVE A REPLY)
Section: Volume A
Explanation/Reference:
Explanation:
Moderate risks are noticeable failure threatening the success of certain goals.
Incorrect Answers:
B: High risk is the significant failure impacting in certain goals not being met.
C: Extremely high risk are the risks that has large impact on enterprise and are most likely results in failure with severe consequences.
D: Low risks are the risk that results in certain unsuccessful goals.

NEW QUESTION: 419
A newly enacted information privacy law significantly increases financial penalties for breaches of personally identifiable information (PII). Which of the following will MOST likely outcome for an organization affected by the new law?
A. Increase in customer complaints
B. Increase in residual risk
C. Increase in compliance breaches
D. Increase in loss event impact
Answer: D (LEAVE A REPLY)

NEW QUESTION: 420
The PRIMARY basis for selecting a security control is:
A. to achieve the desired level of maturity.
B. the cost of the control.
C. the ability to mitigate risk.
D. the materiality of the risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 421
What are the various outputs of risk response?
A. Risk Priority Number
B. Residual risk
C. Risk register updates
D. Project management plan and Project document updates
E. Risk-related contract decisions
Answer: C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The outputs of the risk response planning process are:
Risk Register Updates: The risk register is written in detail so that it can be related to the priority ranking and the planned response.
Risk Related Contract Decisions: Risk related contract decisions are the decisions to transmit risk, such as services, agreements for insurance, and other items as required. It provides a means for sharing risks.
Project Management Plan Updates: Some of the elements of the project management plan updates are:
- Schedule management plan
- Cost management plan
- Quality management plan
- Procurement management plan
- Human resource management plan
- Work breakdown structure
- Schedule baseline
- Cost performance baseline
Project Document Updates: Some of the project documents that can be updated includes:
- Assumption log updates
- Technical documentation updates
Incorrect Answers:
A: Risk priority number is not an output for risk response but instead it is done before applying response.
Hence it acts as one of the inputs of risk response and is not the output of it.
B: Residual risk is not an output of risk response. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk. As, Risk = Threat Vulnerability and Total risk = Threat Vulnerability Asset Value Residual risk can be calculated with the following formula:

Residual Risk = Total Risk - Controls
Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, transferred, mitigated or accepted. They also decide what controls to implement. Any loss due to their decisions falls on their sides.
Residual risk assessments are conducted after mitigation to determine the impact of the risk on the enterprise. For risk assessment, the effect and frequency is reassessed and the impact is recalculated.

NEW QUESTION: 422
Which of the following would be of GREATEST concern to a risk practitioner reviewing current key risk indicators (KRIs)?
A. The KRIs' source data lacks integrity.
B. The KRIs are not quantitative.
C. The KRIs are not automated.
D. The KRIs do not allow for trend analysis.
Answer: (SHOW ANSWER)

NEW QUESTION: 423
Which of the following is MOST important when discussing risk within an organization?
A. Adopting a common risk taxonomy.
B. Creating a risk communication policy.
C. Using key performance indicators (KPIs).
D. Using key risk indicators (KRIs).
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 424
Which of the following is the BEST way to ensure that outsourced service providers comply with the enterprise's information security policy?
A. Penetration testing
B. Service level monitoring
C. Security awareness training

D. Periodic audits
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
As regular audits can spot gaps in information security compliance, periodic audits can ensure that outsourced service provider comply with the enterprise's information security policy.
Incorrect Answers:
A: Penetration testing can identify security vulnerability, but cannot ensure information compliance.
B: Service level monitoring can only identify operational issues in the enterprise's operational environment.
It does not play any role in ensuring that outsourced service provider comply with the enterprise's information security policy.
C: Training can increase user awareness of the information security policy, but is less effective than periodic auditing.

NEW QUESTION: 425
Which of the following is the MOST important factor when deciding on a control to mitigate risk exposure?
A. Comparison against best practice
B. Relevance to the business process
C. Regulatory compliance requirements
D. Cost-benefit analysis
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 426
Which of the following is the BEST way to determine whether new controls mitigate security gaps in a business system?
A. Conduct a compliance check against standards.
B. Perform a vulnerability assessment.
C. Measure the change in inherent risk.
D. Complete an offsite business continuity exercise.
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 427
When of the following is the BEST key control indicator (KCI) to determine the effectiveness of en intrusion prevention system (IPS)?

A. Total number of threats identified
B. Reaction time of the system to threats
C. Percentage of relevant threats mitigated
D. Percentage of system uptime
Answer: C (LEAVE A REPLY)

NEW QUESTION: 428
Which of the following should be a risk practitioner's NEXT step upon learning the organization is not in compliance with a specific legal regulation?
A. Assess the likelihood and magnitude of the associated risk.
B. Identify mitigation activities and compensating controls.
C. Notify senior compliance executives of the associated risk.
D. Determine the penalties for lack of compliance.
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 429
When defining thresholds for control key performance indicators (KPIs). it is MOST helpful to align:
A. information risk assessments with enterprise risk assessments.
B. control performance with risk tolerance of business owners.
C. key risk indicators (KRIs) with risk appetite of the business.
D. the control key performance indicators (KPIs) with audit findings.
Answer: (SHOW ANSWER)

NEW QUESTION: 430
In which of the following risk management capability maturity levels does the enterprise takes major business decisions considering the probability of loss and the probability of reward? Each correct answer represents a complete solution. Choose two.
A. Level 0
B. Level 2
C. Level 5
D. Level 4
E. Explanation:
Enterprise having risk management capability maturity level 4 and 5 takes business decisions considering the probability of loss and the probability of reward, i.e., considering all the aspects of risk.
Answer: C,D,E (LEAVE A REPLY)
is incorrect. Enterprise having risk management capability maturity level 0 takes business decisions without considering risk credential information. Answer:B is incorrect. At this low level of

risk management capability the enterprise take decisions considering specific risk issues within functional and business silos (e.g., security, business continuity, operations).

NEW QUESTION: 431
Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?
A. Risk management plan
B. Project scope statement
C. Risk register
D. Stakeholder register
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The stakeholder register is not an input to the qualitative risk analysis process. The four inputs are the risk register, risk management plan, project scope statement, and organizational process assets.
Incorrect Answers:
A: The Risk management plan is an input to the risk qualitative analysis process.
B: The project scope statement is needed to help with qualitative risk analysis.
C: The risk register can help Wendy to perform qualitative risk analysis.

NEW QUESTION: 432
Which of the following approaches will BEST help to ensure the effectiveness of risk awareness training?
A. Reviewing content with senior management
B. Using reputable third-party training programs
C. Piloting courses with focus groups
D. Creating modules for targeted audiences
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 433
Which of the following would be of GREATEST assistance when justifying investment in risk response strategies?
A. Business impact analysis
B. Resource dependency analysis
C. Total cost of ownership
D. Cost-benefit analysis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 434
Which of the following will BEST ensure that information security risk factors are mitigated when developing in-house applications?
A. Include information security control specifications in business cases.
B. Identify key risk indicators (KRIs) as process output.
C. Identify information security controls in the requirements analysis
D. Design key performance indicators (KPIs) for security in system specifications.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 435
Which of the following statements are true for enterprise's risk management capability maturity level 3?
A. Workflow tools are used to accelerate risk issues and track decisions
B. The business knows how IT fits in the enterprise risk universe and the risk portfolio view
C. The enterprise formally requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals
D. Risk management is viewed as a business issue, and both the drawbacks and benefits of risk are recognized
Answer: A,B,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
An enterprise's risk management capability maturity level is 3 when:
Risk management is viewed as a business issue, and both the drawbacks and benefits of risk are
- recognized.

There is a selected leader for risk management, engaged with the enterprise risk committee, across the
- enterprise.

The business knows how IT fits in the enterprise risk universe and the risk portfolio view.
- Local tolerances drive the enterprise risk tolerance.
- Risk management activities are being aligned across the enterprise.
- Formal risk categories are identified and described in clear terms.
- Situations and scenarios are included in risk awareness training beyond specific policy and structures
- and promote a common language for communicating risk.

Defined requirements exist for a centralized inventory of risk issues.
- Workflow tools are used to accelerate risk issues and track decisions.

Incorrect Answers:

C: Enterprise having risk management capability maturity level 5 requires continuous improvement of risk management skills, based on clearly defined personal and enterprise goals.

NEW QUESTION: 436
John works as a project manager for BlueWell Inc. He is determining which risks can affect the project. Which of the following inputs of the identify risks process is useful in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk?
A. Activity duration estimates
B. Activity cost estimates
C. Risk management plan
D. Schedule management plan
Answer: A (LEAVE A REPLY)
Section: Volume C
Explanation:
The activity duration estimates review is valuable in identifying risks associated to the time allowances for the activities or projects as a whole, with a width of the range indicating the degrees of risk.
Incorrect Answers:
B: The activity cost estimates review is valuable in identifying risks as it provides a quantitative assessment of the expected cost to complete scheduled activities and is expressed as a range, with a width of the range indicating the degrees of risk.
C: A Risk management plan is a document arranged by a project manager to estimate the effectiveness, predict risks, and build response plans to mitigate them. It also consists of the risk assessment matrix.
D: It describes how the schedule contingencies will be reported and assessed.

NEW QUESTION: 437
You are the project manager of the AFD project for your company. You are working with the project team to reassess existing risk events and to identify risk events that have not happened and whose relevancy to the project has passed. What should you do with these events that have not happened and would not happen now in the project?

A. Add the risk to the issues log
B. Close the outdated risks
C. Add the risks to the risk register
D. Add the risks to a low-priority watch-list
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Risks that are now outdated should be closed by the project manager, there is no need to keep record of that.
Incorrect Answers:
A: Risks do not go into the issue log, but the risk register.
C: Identified risks are already in the risk register.
D: Risks with low probability and low impact go on the risk watchlist.

NEW QUESTION: 438
Which of the following provides the BEST measurement of an organization's risk management maturity level?
A. IT alignment to business objectives
B. The results of a gap analysis
C. Key risk indicators (KRIs)
D. Level of residual risk
Answer: (SHOW ANSWER)

NEW QUESTION: 439
You are the project manager for your organization. You are preparing for the quantitative risk analysis.
Mark, a project team member, wants to know why you need to do quantitative risk analysis when you just completed qualitative risk analysis. Which one of the following statements best defines what quantitative risk analysis is?
A. Quantitative risk analysis is the review of the risk events with the high probability and the highest impact on the project objectives.
B. Quantitative risk analysis is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
C. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.
D. Quantitative risk analysis is the planning and quantification of risk responses based on probability and impact of each risk event.
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:

Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives. It is performed on risk that have been prioritized through the qualitative risk analysis process.
Incorrect Answers:
A: While somewhat true, this statement does not completely define the quantitative risk analysis process.
B: This is actually the definition of qualitative risk analysis.
D: This is not a valid statement about the quantitative risk analysis process. Risk response planning is a separate project management process.

NEW QUESTION: 440
The PRIMARY objective for selecting risk response options is to:
A. minimize residual risk.
B. reduce risk factors.
C. reduce risk to an acceptable level.
D. identify compensating controls.
Answer: C (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 441
Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?
A. Risk management plan
B. Project scope statement
C. Risk register
D. Stakeholder register
E. Explanation:
The stakeholder register is not an input to the qualitative risk analysis process. The four inputs are
the risk register, risk management plan, project scope statement, and organizational process assets.
F. is incorrect. The risk register can help Wendy to perform qualitative risk analysis.
G. is incorrect. The project scope statement is needed to help with qualitative risk analysis.
Answer: D,E,F,G (LEAVE A REPLY)
is incorrect. The Risk management plan is an input to the risk qualitative analysis process.

NEW QUESTION: 442
Which of the following is the MOST important data source for monitoring key risk indicators (KRIs)?
A. Audit reports from internal information systems audits

B. Directives from legal and regulatory authorities
C. Trend analysis of external risk factors
D. Automated logs collected from different systems
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 443
In which of the following conditions business units tend to point the finger at IT when projects are not delivered on time?
A. Threat identification in project
B. System failure
C. Misalignment between real risk appetite and translation into policies
D. Existence of a blame culture
Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation:
In a blame culture, business units tend to point the finger at IT when projects are not delivered on time or do not meet expectations. In doing so, they fail to realize how the business unit's involvement up front affects project success. In extreme cases, the business unit may assign blame for a failure to meet the expectations that the unit never clearly communicated.
Incorrect Answers:
A, B, C: These are not relevant to the pointing of finger at IT when projects are not delivered on time.

NEW QUESTION: 444
Who is MOST likely to be responsible for the coordination between the IT risk strategy and the business risk strategy?
A. Chief financial officer
B. Information security director
C. Chief information officer
D. Internal audit director
Answer: C (LEAVE A REPLY)

NEW QUESTION: 445
Which of the following provides the MOST up-to-date information about the effectiveness of an organization's overall IT control environment?
A. Internal audit findings
B. Risk heat maps
C. Key performance indicators (KPIs)
D. Periodic penetration testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 446
Which of the following is the BEST method for assessing control effectiveness against technical vulnerabilities that could be exploited to compromise an information system?
A. Vulnerability scanning
B. Penetration testing
C. Systems log correlation analysis
D. Monitoring of intrusion detection system (IDS) alerts
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 447
Which of the following is the HIGHEST risk of a policy that inadequately defines data and system ownership?
A. User management coordination does not exists
B. Audit recommendations may not be implemented
C. Users may have unauthorized access to originate, modify or delete data
D. Specific user accountability cannot be established
E. Explanation:
There is an increased risk without a policy defining who has the responsibility for granting access to specific data or systems, as one could gain system access without a justified business needs. There is better chance that business objectives will be properly supported when there is appropriate ownership.
Answer: C (LEAVE A REPLY)
B, and D are incorrect. These risks are not such significant as compared to unauthorized access.

NEW QUESTION: 448
An organization has engaged a third party to provide an Internet gateway encryption service that protects sensitive data uploaded to a cloud service. This is an example of risk:
A. transfer
B. acceptance
C. mitigation
D. avoidance
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 449
Which of the following will help ensure the elective decision-making of an IT risk management committee?

A. Committee meets at least quarterly
B. Key stakeholders are enrolled as members
C. Approved minutes ate forwarded to senior management
D. Functional overlap across the business is minimized
Answer: (SHOW ANSWER)

NEW QUESTION: 450
The number of tickets to rework application code has significantly exceeded the established threshold. Which of the following would be the risk practitioner's BEST recommendation?
A. Implement training on coding best practices
B. Perform a code review
C. Perform a root cause analysis
D. Implement version control software
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 451
You are the project manager of a SGT project. You have been actively communicating and working with the project stakeholders. One of the outputs of the "manage stakeholder expectations" process can actually create new risk events for your project. Which output of the manage stakeholder expectations process can create risks?
A. Project management plan updates
B. An organizational process asset updates
C. Change requests
D. Project document updates
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The manage stakeholder expectations process can create change requests for the project, which can cause new risk events to enter into the project.
Change requests are requests to expand or reduce the project scope, modify policies, processes, plans, or procedures, modify costs or budgets or revise schedules. These requests for a change can be direct or indirect, externally or internally initiated, and legally or contractually imposed or optional. A Project Manager needs to ensure that only formally documented requested changes are processed and only approved change requests are implemented.
Incorrect Answers:
A: The project management plan updates do not create new risks.
B: The organizational process assets updates do not create new risks.
D: The project document updates do not create new risks.

NEW QUESTION: 452
Which of the following is the MOST important responsibility of a risk owner?
A. Accepting residual risk
B. Establishing business information criteria
C. Establishing the risk register
D. Testing control design
Answer: A (LEAVE A REPLY)

NEW QUESTION: 453
You are preparing to complete the quantitative risk analysis process with your project team and several subject matter experts. You gather the necessary inputs including the project's cost management plan. Why is it necessary to include the project's cost management plan in the preparation for the quantitative risk analysis process?
A. The project's cost management plan provides control that may help determine the structure for quantitative analysis of the budget.
B. The project's cost management plan can help you to determine what the total cost of the project is allowed to be.
C. The project's cost management plan provides direction on how costs may be changed due to identified risks.
D. The project's cost management plan is not an input to the quantitative risk analysis process.
E. Explanation:
The cost management plan is an input to the quantitative risk analysis process because of the cost management control it provides. The cost management plan sets how the costs on a project are managed during the project's lifecycle. It defines the format and principles by which the project costs are measured, reported, and controlled. The cost management plan identifies the person responsible for managing costs, those who have the authority to approve changes to the project or its budget, and how cost performance is quantitatively calculated and reported upon.
Answer: A (LEAVE A REPLY)
is incorrect. This is not a valid statement. The cost management plan is an input to the quantitative risk analysis process. Answer:B is incorrect. The cost management plan defines the estimating, budgeting, and control of the project's cost. Answer:C is incorrect. While the cost management plan does define the cost change control system, this is not the best answer for this

NEW QUESTION: 454
An audit reveals that several terminated employee accounts maintain access. Which of the following should be the FIRST step to address the risk?
A. Perform a risk assessment
B. Disable user access
C. Perform root cause analysis
D. Develop an access control policy
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 455
An identified high probability risk scenario involving a critical, proprietary business function has an annualized cost of control higher than the annual loss expectancy. Which of the following is the BEST risk response?
A. Avoid
B. Transfer
C. Accept
D. Mitigate
Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 456
When defining thresholds for control key performance indicators (KPIs), it is MOST helpful to align:
A. key risk indicators (KRIs) with risk appetite of the business
B. the control key performance indicators (KPIs) with audit findings
C. control performance with risk tolerance of business owners
D. information risk assessments with enterprise risk assessments
Answer: B (LEAVE A REPLY)
Section: Volume D
Explanation

NEW QUESTION: 457
Improvements in the design and implementation of a control will MOST likely result in an update to:
A. risk tolerance
B. inherent risk.
C. risk appetite
D. residual risk.
Answer: (SHOW ANSWER)

NEW QUESTION: 458
Which of the following is NOT true for effective risk communication?
A. Risk information must be known and understood by all stakeholders.
B. Use of technical terms of risk
C. Any communication on risk must be relevant
D. For each risk, critical moments exist between its origination and its potential business consequence
E. Explanation:
For effective communication, information communicated should not inundate the recipients. All ground rules of good communication apply to communication on risk. This includes the avoidance of jargon and technical terms regarding risk because the intended audiences are generally not deeply technologically skilled. Hence use of technical terms is avoided for effective communication
Answer: B (LEAVE A REPLY)
C, and D are incorrect. These all are true for effective risk communication. For effective risk communication the risk information should be clear, concise, useful and timely. Risk information must be known and understood by all the stakeholders. Information or communication should not overwhelm the recipients. This includes the avoidance of technical terms regarding risk because the intended audiences are generally not much technologically skilled. Any communication on risk must be relevant. Technical information that is too detailed or is sent to inappropriate parties will hinder, rather than enable, a clear view of risk. For each risk, critical moments exist between its origination and its potential business consequence. Information should also be aimed at the correct target audience and available on need-to-know basis. Hence for effective risk communication risk information should be: Clear Concise Useful Timely given Aimed at the correct audience Available on need-to-know basis

NEW QUESTION: 459
Which of the following is the MOST important aspect to ensure that an accurate risk register is maintained?
A. Publish the risk register in a knowledge management platform with workflow features that periodically contacts and polls risk assessors to ensure accuracy of content
B. Perform regular audits by audit personnel and maintain risk register
C. Submit the risk register to business process owners for review and updating
D. Monitor key risk indicators, and record the findings in the risk register
Answer: A (LEAVE A REPLY)
Section: Volume D
Explanation:
A knowledge management platform with workflow and polling feature will automate the process of maintaining the risk registers. Hence this ensures that an accurate and updated risk register is maintained.
Incorrect Answers:

B: Audit personnel may not have the appropriate business knowledge in risk assessment, hence cannot properly identify risk. Regular audits may also cause hindrance to the business activities.
C: Business process owners typically cannot effectively identify risk to their business processes. They may not have the ability to be unbiased and may not have the appropriate skills or tools for evaluating risks.
D: Monitoring key risk indicators, and record the findings in the risk register will only provide insights to known and identified risk and will not account for obscure risk, i.e. , risk that has not been identified yet.

NEW QUESTION: 460
After a risk has been identified, who is in the BEST position to select the appropriate risk treatment option?
A. The business process owner
B. The risk practitioner
C. The control owner
D. The risk owner
Answer: (SHOW ANSWER)

NEW QUESTION: 461
You are the project manager for BlueWell Inc. You have noticed that the risk level in your project increases above the risk tolerance level of your enterprise. You have applied several risk response. Now you have to update the risk register in accordance to risk response process. All of the following are included in the risk register except for which item?
A. Risk triggers
B. Agreed-upon response strategies
C. Network diagram analysis of critical path activities
D. Risk owners and their responsibility
Answer: C (LEAVE A REPLY)
The risk register does not examine the network diagram and the critical path. There may be risks associated with the activities on the network diagram, but it does not address the network diagram directly. The risk register is updated at the end of the plan risk response process with the information that was discovered during the process. The response plans are recorded in the risk register. In the risk register, risk is stated in order of priority, i.e., those with the highest potential for threat or opportunity first. Some risks might not require response plans at all, but then too they should be put on a watch list and monitored throughout the project. Following elements should appear in the risk register: List of identified risks, including their descriptions, root causes, and how the risks impact the project objectives Risk owners and their responsibility Outputs from the Perform Qualitative Analysis process Agreed-upon response strategies Risk triggers Cost and schedule activities needed to implement risk responses Contingency plans Fallback plans, which are risk response plans that are executed when the initial risk response plan proves to be ineffective Contingency reserves Residual risk, which is a leftover risk that remains after the risk

response strategy has been implemented Secondary risks, which are risks that come about as a result of implementing a risk response

NEW QUESTION: 462
An organization has decided to use an external auditor to review the control environment of an outsourced service provider. The BEST control criteria to evaluate the provider would be based on:
A. the service provider's existing controls
B. a recognized industry control framework
C. guidance provided by the external auditor
D. The organization's specific control requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 463
Mortality tables are based on what mathematical activity?
Each correct answer represents a complete solution. Choose three.
A. Normal distributions
B. Probabilities
C. Impact
D. Sampling
E. Explanation:
Probability identifies the chances that a particular event will happen under certain circumstances. The variables provided are based on information gathered in real life. For situations with large numbers, a smaller set of participants are identified to represent the larger population. This represents a sample of the population. The points are mapped to identify their distribution. Normal distribution refers to the theoretical plotting of points against the mathematical mean. The result of these activities provides a reasonable predictability for the mortality of the subject.
Answer: A,B,D,E (LEAVE A REPLY)
is incorrect. Impact is used to identify the magnitude of identified risks. The risk leads to some type of loss. However, instead of quantifying the loss as a dollar value, an impact assessment could use words such as Low, Medium, or High. Hence it is not mathematical.

NEW QUESTION: 464
You are the project manager of HFD project. You have identified several project risks. You have adopted alternatives to deal with these risks which do not attempt to reduce the probability of a risk event or its impacts.
Which of the following response have you implemented?
A. Acceptance
B. Mitigation
C. Avoidance
D. Contingent response

Answer: D (LEAVE A REPLY)
Section: Volume D
Explanation
Explanation:
Contingent response strategy, also known as contingency planning, involves adopting alternatives to deal with the risks in case of their occurrence. Unlike the mitigation planning in which mitigation looks to reduce the probability of the risk and its impact, contingency planning doesn't necessarily attempt to reduce the probability of a risk event or its impacts. Contingency comes into action when the risk event actually occurs.
Incorrect Answers:
A: Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive and active.
* Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
* Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
B: Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. The main control types are:
* Managerial(e.g.,policies)
* Technical (e.g., tools such as firewalls and intrusion detection systems)
* Operational (e.g., procedures, separation of duties)
* Preparedness activities
C: Risk avoidance means to evade risk altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event.

NEW QUESTION: 465
Which of the following BEST indicates the condition of a risk management program?
A. Number of risk register entries
B. Level of financial support
C. Number of controls
D. Amount of residual risk
Answer: A (LEAVE A REPLY)

NEW QUESTION: 466
Senior management wants to increase investment in the organization's cybersecurity program in response to changes in the external threat landscape. Which of the following would BEST help to prioritize investment efforts?
A. Reviewing the outcome of the latest security risk assessment

B. Analyzing cyber intelligence reports
C. Increasing the frequency of updates to the risk register
D. Engaging independent cybersecurity consultants
Answer: (SHOW ANSWER)

NEW QUESTION: 467
Which of the following is the PRIMARY reason to adopt key control indicators (KCIs) in the risk monitoring and reporting process?
A. To provide assurance of adherence to risk management policies
B. To provide measurements on the potential for risk to occur
C. To provide assessments of mitigation effectiveness
D. To provide data for establishing the risk profile
Answer: C (LEAVE A REPLY)

NEW QUESTION: 468
Which of the following is the GREATEST risk associated with an environment that lacks documentation of the architecture?
A. Overlapping threats
B. Legacy technology systems
C. Network isolation
D. Unknown vulnerabilities
Answer: A (LEAVE A REPLY)

NEW QUESTION: 469
Which of the following will BEST help to ensure key risk indicators (KRIs) provide value to risk owners?
A. Timely notification
B. Cost minimization
C. Ongoing training
D. Return on investment (ROI)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 470
After mapping generic risk scenarios to organizational security policies, the NEXT course of action should be to:
A. validate the risk scenarios for business applicability.
B. reduce the number of risk scenarios to a manageable set.
C. record risk scenarios in the risk register for analysis.
D. perform a risk analysis on the risk scenarios.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 471
Which of the following is the MOST important consideration for protecting data assets m a Business application system?
A. Encrypted communication is established between applications and data servers
B. Application controls are aligned with data classification lutes
C. Offsite encrypted backups are automatically created by the application
D. Application users are periodically trained on proper data handling practices
Answer: (SHOW ANSWER)

NEW QUESTION: 472
You work as the project manager for Bluewell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decide, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project, what is likely to increase?
A. Human resource needs
B. Quality control concerns
C. Costs
D. Risks
E. Explanation:
Fast tracking allows entire phases of the project to overlap and generally increases risks within the
project.
Fast tracking is a technique for compressing project schedule. In fast tracking, phases are overlapped that would normally be done in sequence. It is shortening the project schedule without reducing the project scope.
F. is incorrect. Quality control concerns usually are not affected by fast tracking decisions.
G. is incorrect. Costs do not generally increase based on fast tracking decisions.
Answer: D,E,F,G (LEAVE A REPLY)
is incorrect. Human resources are not affected by fast tracking in most scenarios.

NEW QUESTION: 473

You are the project manager of GHT project. You and your team have developed risk responses for those risks with the highest threat to or best opportunity for the project objectives. What are the immediate steps you should follow, after planning for risk response process? Each correct answer represents a complete solution.
Choose three.
A. Updating Project management plan and Project document
B. Applying controls
C. Updating Risk register
D. Prepare Risk-related contracts
Answer: (SHOW ANSWER)
Section: Volume C
Explanation:
The risk register is updated at the end of the plan risk response process with the information that was discovered during the process. The response plans are recorded in the risk register.
Project management plan consisting of WBS, schedule baseline and cost performance baseline should be updated. After planning risk response process, there may be requirement of updating project documents like technical documentation and assumptions, documented in the project scope statement.
If risk response strategies include responses such as transference or sharing, it may be necessary to purchase services or items from third parties. Contracts for those services can be prepared and discussed with the appropriate parties.
Incorrect Answers:
B: Controls are implemented in the latter stage of risk response process. It is not immediate task after the planning of risk response process, as updating of several documents is done first.
The purpose of the Plan Risk Responses process is to develop risk responses for those risks with the highest threat to or best opportunity for the project objectives. The Plan Risk Responses process has four outputs:
* Risk register updates
* Risk-related contract decisions
* Project management plan updates
* Project document updates

NEW QUESTION: 474
Which of the following BEST indicates that an organization has implemented IT performance requirements?
A. Benchmarking data
B. Vendor references
C. Accountability matrix
D. Service level agreements (SLA)
Answer: (SHOW ANSWER)

NEW QUESTION: 475
Which of the following is MOST helpful in preventing risk events from materializing?
A. Establishing key risk indicators (KRIs)
B. Maintaining the risk register
C. Reviewing and analyzing security incidents
D. Prioritizing and tracking issues
Answer: D (LEAVE A REPLY)

NEW QUESTION: 476
Of the following, who is BEST suited to assist a risk practitioner in developing a relevant set of risk scenarios?
A. Control owner
B. Asset owner
C. Internal auditor
D. Finance manager
Answer: B (LEAVE A REPLY)

NEW QUESTION: 477
A monthly payment report is generated from the enterprise resource planning (ERP) software to validate data against the old and new payroll systems. What is the BEST way to mitigate the risk associated with data integrity loss in the new payroll system after data migration?
A. Compare encrypted data with checksums.
B. Compare new system reports with functional requirements.
C. Compare processing output from both systems using the previous month's data.
D. Compare results of user acceptance testing (UAT) with the testing criteria.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 478
What are the various outputs of risk response?
A. Risk Priority Number
B. Residual risk
C. Risk register updates
D. Project management plan and Project document updates
E. Risk-related contract decisions
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The outputs of the risk response planning process are:
Risk Register Updates: The risk register is written in detail so that it can be related to the priority ranking and the planned response.

Risk Related Contract Decisions: Risk related contract decisions are the decisions to transmit risk, such
as services, agreements for insurance, and other items as required. It provides a means for sharing risks.
Project Management Plan Updates: Some of the elements of the project management plan updates
are:
- Schedule management plan
- Cost management plan
- Quality management plan
- Procurement management plan
- Human resource management plan
- Work breakdown structure
- Schedule baseline
- Cost performance baseline
Project Document Updates: Some of the project documents that can be updated includes:
- Assumption log updates
- Technical documentation updates
Incorrect Answers:
A: Risk priority number is not an output for risk response but instead it is done before applying response.
Hence it acts as one of the inputs of risk response and is not the output of it.
B: Residual risk is not an output of risk response. Residual risk is the risk that remains after applying controls. It is not feasible to eliminate all risks from an organization. Instead, measures can be taken to reduce risk to an acceptable level. The risk that is left is residual risk. As, Risk = Threat Vulnerability and Total risk = Threat Vulnerability Asset Value Residual risk can be calculated with the following formula:
Residual Risk = Total Risk - Controls
Senior management is responsible for any losses due to residual risk. They decide whether a risk should be avoided, transferred, mitigated or accepted. They also decide what controls to implement. Any loss due to their decisions falls on their sides.
Residual risk assessments are conducted after mitigation to determine the impact of the risk on the enterprise. For risk assessment, the effect and frequency is reassessed and the impact is recalculated.

NEW QUESTION: 479
You are the risk official of your enterprise. You have just completed risk analysis process. You noticed that the risk level associated with your project is less than risk tolerance level of your enterprise. Which of following is the MOST likely action you should take?
A. Apply risk response

B. Update risk register
C. No action
D. Prioritize risk response options
Answer: C (LEAVE A REPLY)
Section: Volume B
Explanation:
When the risk level is less than risk tolerance level of the enterprise than no action is taken against that, because the cost of mitigation will increase over its benefits.
Incorrect Answers:
A: This is not a valid answer, as no response is being applied to such low risk level.
B: Risk register is updates after applying response, and as no response is applied to such low risk level; hence no updating is done.
D: This is not a valid answer, as no response is being applied to such low risk level.

NEW QUESTION: 480
Which of the following phases is involved in the Data Extraction, Validation, Aggregation and Analysis?
A. Risk response and Risk monitoring
B. Requirements gathering, Data access, Data validation, Data analysis, and Reporting and corrective action
C. Data access and Data validation
D. Risk identification, Risk assessment, Risk response and Risk monitoring
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The basic concepts related to data extraction, validation, aggregation and analysis is important as KRIs often rely on digital information from diverse sources. The phases which are involved in this are:
Requirements gathering: Detailed plan and project's scope is required for monitoring risks. In the case
- of a monitoring project, this step should involve process owners, data owners, system custodians and other process stakeholders.
Data access: In the data access process, management identifies which data are available and how
- they can be acquired in a format that can be used for analysis. There are two options for data extraction:
- Extracting data directly from the source systems after system owner approval
- Receiving data extracts from the system custodian (IT) after system owner approval Direct extraction is preferred, especially since this involves management monitoring its own controls, instead of auditors/third parties monitoring management's controls. If it is not feasible to get direct

access, a data access request form should be submitted to the data owners that detail the appropriate data fields to be extracted. The request should specify the method of delivery for the file.
Data validation: Data validation ensures that extracted data are ready for analysis. One of its important
objective is to perform tests examining the data quality to ensure data are valid complete and free of errors. This may also involve making data from different sources suitable for comparative analysis.
Following concepts should be considered while validating data:
- Ensure the validity, i.e., data match definitions in the table layout
- Ensure that the data are complete
- Ensure that extracted data contain only the data requested
- Identify missing data, such as gaps in sequence or blank records
- Identify and confirm the validity of duplicates
- Identify the derived values
- Check if the data given is reasonable or not
- Identify the relationship between table fields
- Record, in a transaction or detail table, that the record has no match in a master table Data analysis: Analysis of data involves simple set of steps or complex combination of commands and
other functionality. Data analysis is designed in such a way to achieve the stated objectives from the project plan. Although this may be applicable to any monitoring activity, it would be beneficial to consider transferability and scalability. This may include robust documentation, use of software development standards and naming conventions.
Reporting and corrective action: According to the requirements of the monitoring objectives and the
technology being used, reporting structure and distribution are decided. Reporting procedures indicate to whom outputs from the automated monitoring process are distributed so that they are directed to the right people, in the right format, etc. Similar to the data analysis stage, reporting may also identify areas in which changes to the sensitivity of the reporting parameters or the timing and frequency of the monitoring activity may be required.
Incorrect Answers:
D: These are the phases that are involved in risk management.

NEW QUESTION: 481
Mary is the project manager for the BLB project. She has instructed the project team to assemble, to review the risks. She has included the schedule management plan as an input for the quantitative risk analysis process. Why is the schedule management plan needed for quantitative risk analysis?
A. Mary will schedule when the identified risks are likely to happen and affect the project schedule.

B. Mary will utilize the schedule controls and the nature of the schedule for the quantitative analysis of the schedule.
C. Mary will use the schedule management plan to schedule the risk identification meetings throughout the remaining project.
D. Mary will utilize the schedule controls to determine how risks may be allowed to change the project schedule.
E. Explanation:
The controls within the schedule management plan can shape how quantitative risk analysis will be performed on the schedule. Schedule management plan also describes how the schedule contingencies will be reported and assessed.
Answer: (SHOW ANSWER)
is incorrect. This is not a valid answer for this questionthroughout theproject, but it is not scheduled during the quantitative risk analysis process. Answer: A is incorrect. When risks are likely to happen is important, but it is not the best answer for thisquestionoption D is incorrect. Risks may affect the project schedule, but this is not the best answer for thequestion.

NEW QUESTION: 482
Which of the following is the BEST evidence that a user account has been properly authorized?
A. Notification from human resources that the account is active
B. Formal approval of the account by the user's manager
C. User privileges matching the request form
D. An email from the user accepting the account
Answer: (SHOW ANSWER)
Section: Volume D
Explanation/Reference:

NEW QUESTION: 483
You are working on a project in an enterprise. Some part of your project requires e-commerce, but your enterprise choose not to engage in e-commerce. This scenario is demonstrating which of the following form?
A. risk avoidance
B. risk treatment

C. risk acceptance
D. risk transfer
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Each business process involves inherent risk. Not engaging in any activity avoids the inherent risk associated with the activity. Hence this demonstrates risk avoidance.
Incorrect Answers:
B: Risk treatment means that action is taken to reduce the frequency and impact of a risk.
C: Acceptance means that no action is taken relative to a particular risk, and loss is accepted when/if it occurs. This is different from being ignorant of risk; accepting risk assumes that the risk is known, i.e., an informed decision has been made by management to accept it as such.
D: Risk transfer/sharing means reducing either risk frequency or impact by transferring or otherwise sharing a portion of the risk. Common techniques include insurance and outsourcing. These techniques do not relieve an enterprise of a risk, but can involve the skills of another party in managing the risk and reducing the financial consequence if an adverse event occurs.

NEW QUESTION: 484
David is the project manager of the HRC Project. He has identified a risk in the project, which could cause the delay in the project. David does not want this risk event to happen so he takes few actions to ensure that the risk event will not happen. These extra steps, however, cost the project an additional $10,000. What type of risk response has David adopted?
A. Avoidance
B. Mitigation
C. Acceptance
D. Transfer
Answer: (SHOW ANSWER)
Section: Volume A
Explanation:
As David is taking some operational controls to reduce the likelihood and impact of the risk, hence he is adopting risk mitigation. Risk mitigation means that actions are taken to reduce the likelihood and/or impact of risk.
Incorrect Answers:
A: Risk avoidance means that activities or conditions that give rise to risk are discontinued. But here, no such actions are taken, therefore risk in not avoided.
C: Risk acceptance means that no action is taken relative to a particular risk; loss is accepted in case it occurs.
As David has taken some actions in case to defend, therefore he is not accepting risk.
D: David has not hired a vendor to manage the risk for his project; therefore he is not transferring the risk.

NEW QUESTION: 485
An organization has granted a vendor access to its data in order to analyze customer behavior. Which of the following would be the MOST effective control to mitigate the risk of customer data leakage?
A. Restrict access to customer data on a "need to know" basis
B. Enforce criminal background checks
C. Mask customer data fields
D. Require vendor to sign a confidentiality agreement
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 486
When formulating a social media policy lo address information leakage, which of the following is the MOST important concern to address?
A. Sharing personal information on social media
B. Sharing company information on social media
C. Using social media to maintain contact with business associates
D. Using social media for personal purposes during working hours
Answer: (SHOW ANSWER)

NEW QUESTION: 487
If one says that the particular control or monitoring tool is sustainable, then it refers to what ability?
A. The ability to adapt as new elements are added to the environment
B. The ability to ensure the control remains in place when it fails
C. The ability to protect itself from exploitation or attack
D. The ability to be applied in same manner throughout the organization
Answer: (SHOW ANSWER)
Section: Volume D
Explanation/Reference:
Explanation:
Sustainability of the controls or monitoring tools refers to its ability to function as expected over time or when changes are made to the environment.
Incorrect Answers:
B: Sustainability ensures that controls changes with the conditions, so as not to fail in any circumstances.
Hence this in not a valid answer.
C: This is not a valid answer.
D: This is not a valid definition for defining sustainability of a tool.

NEW QUESTION: 488

Which of the following approaches to bring you own device (BYOD) service delivery provides the BEST protection from data loss?

A. Penetration testing and session timeouts

B. Implement remote monitoring

C. Enforce strong passwords and data encryption

D. Enable data wipe capabilities

Answer: B (LEAVE A REPLY)

Section: Volume D

NEW QUESTION: 489

An organization has recently updated its disaster recovery plan (DRP). Which of the following would be the GREATEST risk if the new plan is not tested?

A. Recovery costs may increase significantly.

B. External resources may need to be involved.

C. Data privacy regulations may be violated.

D. Service interruptions may be longer than anticipated.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 490

Which of the following is MOST important when developing key performance indicators (KPIs)?

A. Alignment to management reports

B. Alignment to risk responses

C. Alerts when risk thresholds are reached

D. Identification of trends

Answer: (SHOW ANSWER)

Explanation/Reference:

Explanation:

Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.

Reference: https://m.isaca.org/Certification/Additional-Resources/Documents/CRISC-Item-Development- Guide_bro_Eng_0117.pdf

NEW QUESTION: 491

A global organization is planning to collect customer behavior data through social media advertising. Which of the following is the MOST important business risk to be considered?

A. Business advertising will need to be tailored by country.

B. Data sampling may be impacted by various industry restrictions.

C. The data analysis may be ineffective in achieving objectives.

D. Regulatory requirements may differ in each country.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 492
You are the risk official in Techmart Inc. You are asked to perform risk assessment on the impact of losing a network connectivity for 1 day. Which of the following factors would you include?
A. Aggregate compensation of all affected business users.
B. Hourly billing rate charged by the carrier
C. Value that enterprise get on transferring data over the network
D. Financial losses incurred by affected business units
Answer: D (LEAVE A REPLY)
Section: Volume B
Explanation:
The impact of network unavailability is the cost it incurs to the enterprise. As the network is unavailable for 1 day, it can be considered as the failure of some business units that rely on this network. Hence financial losses incurred by this affected business unit should be considered.
Incorrect Answers:
A, B, C: These factors in combination contribute to the overall financial impact, i.e., financial losses incurred by affected business units.

NEW QUESTION: 493
When using a third party to perform penetration testing, which of the following is the MOST important control to minimize operational impact?
A. Clearly define the project scope
B. Require the vendor to have liability insurance.
C. Perform a background check on the vendor.
D. Require the vendor to sign a nondisclosure agreement.
Answer: (SHOW ANSWER)

NEW QUESTION: 494
You are working in an enterprise. You project deals with important files that are stored on the computer. You have identified the risk of the failure of operations. To address this risk of failure, you have guided the system administrator sign off on the daily backup. This scenario is an example of which of the following?
A. Risk avoidance
B. Risk transference
C. Risk acceptance
D. Risk mitigation
E. Explanation:
Mitigation is the strategy that provides for the definition and implementation of controls to address the risk described. Here in this scenario, you are trying to reduce the risk of operation failure by guiding administrator to take daily backup, hence it is risk mitigation.
Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. The main

control types are:
Managerial(e.g.,policies)
Technical (e.g., tools such as firewalls and intrusion detection systems)
Operational (e.g., procedures, separation of duties)
Preparedness activities
F. is incorrect. The scenario does not describe the sharing of risk. Transference is the strategy that provides for sharing risk with partners or taking insurance coverage.
G. is incorrect. The scenario does not describe risk avoidance. Avoidance is a strategy that provides for not implementing certain activities or processes that would incur risk.
Answer: (SHOW ANSWER)
is incorrect. The scenario does not describe risk acceptance, Acceptance is a strategy that provides for formal acknowledgement of the existence of a risk and the monitoring of that risk.

NEW QUESTION: 495
Which of the following BEST ensures that a firewall is configured in compliance with an enterprise's security policy?
A. Interview the firewall administrator.
B. Review the actual procedures.
C. Review the device's log file for recent attacks.
D. Review the parameter settings.
E. Explanation:
A review of the parameter settings will provide a good basis for comparison of the actual configuration to the security policy and will provide reliable audit evidence documentation.
Answer: D,E (LEAVE A REPLY)
is incorrect. While procedures may provide a good understanding of how the firewall is supposed to be managed, they do not reliably confirm that the firewall configuration complies with the enterprise's security policy. Answer: A is incorrect. While interviewing the firewall administrator may provide a good process overview, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy. Answer: C is incorrect. While reviewing the device's log file for recent attacks may provide indirect evidence about the fact that logging is enabled, it does not reliably confirm that the firewall configuration complies with the enterprise's security policy.

NEW QUESTION: 496
Which of the following events refer to loss of integrity?
Each correct answer represents a complete solution. Choose three.
A. Someone sees company's secret formula
B. Someone makes unauthorized changes to a Web site
C. An e-mail message is modified in transit
D. A virus infects a file

Answer: B,C,D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Loss of integrity refers to the following types of losses:
An e-mail message is modified in transit A virus infects a file
- Someone makes unauthorized changes to a Web site
-
Incorrect Answers:
A: Someone sees company's secret formula or password comes under loss of confidentiality.

NEW QUESTION: 497
Which of The following is the PRIMARY consideration when establishing an organization's risk management methodology?
A. Risk tolerance level
B. Benchmarking information
C. Business context
D. Resource requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 498
You work as a project manager for BlueWell Inc. You have declined a proposed change request because of the risk associated with the proposed change request. Where should the declined change request be documented and stored?
A. Change request log
B. Project archives
C. Lessons learned
D. Project document updates
Answer: (SHOW ANSWER)
Section: Volume D
Explanation:
The change request log records the status of all change requests, approved or declined.

The change request log is used as an account for change requests and as a means of tracking their disposition on a current basis. The change request log develops a measure of consistency into the change management process. It encourages common inputs into the process and is a common estimation approach for all change requests. As the log is an important component of project requirements, it should be readily available to the project team members responsible for project delivery. It should be maintained in a file with read-only access to those who are not responsible for approving or disapproving project change requests.
Incorrect Answers:
B: The project archive includes all project documentation and is created through the close project or phase process. It is not the best choice for this question.
C: Lessons learned are not the correct place to document the status of a declined, or approved, change request.
D: The project document updates is not the best choice for this to be fleshed into the project documents, but the declined changes are part of the change request log.

NEW QUESTION: 499
Jeff works as a Project Manager for www.company.com Inc. He and his team members are involved in the identify risk process. Which of the following tools & techniques will Jeff use in the identify risk process?
Each correct answer represents a complete solution. (Choose three.)
A. Information gathering technique
B. Documentation reviews
C. Checklist analysis
D. Risk categorization
Answer: A,B,C (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The various tools & techniques used in the identify risk process are as follows:
Documentation reviews
Information gathering technique
Checklist analysis
Assumption analysis
Diagramming techniques
SWOT analysis
Expert judgment

NEW QUESTION: 500
The MAIN purpose of having a documented risk profile is to:
A. keep the risk register up-to-date.

B. comply with external and internal requirements.
C. prioritize investment projects.
D. enable well-informed decision making.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 501
An IT risk practitioner has been asked to regularly report on the overall status and effectiveness of the IT risk management program. Which of the following is MOST useful for this purpose?
A. Capability maturity level
B. Control self-assessment (CSA)
C. Internal audit plan
D. Balanced scorecard
Answer: D (LEAVE A REPLY)

NEW QUESTION: 502
Mary is a project manager in her organization. On her current project she is working with her project team and other key stakeholders to identify the risks within the project. She is currently aiming to create a comprehensive list of project risks so she is using a facilitator to help generate ideas about project risks. What risk identification method is Mary likely using?
A. Delphi Techniques
B. Expert judgment
C. Brainstorming
D. Checklist analysis
E. Explanation:
Mary is using brainstorming in this example. Brainstorming attempts to create a comprehensive list of risks and often is led by a moderator or facilitator to move the process along. Brainstorming is a technique to gather general data. It can be used to identify risks, ideas, or solutions to issues by using a group of team members or subject-matter expert. Brainstorming is a group creativity technique that also provides other benefits, such as boosting morale, enhancing work enjoyment, and improving team work.
Answer: C (LEAVE A REPLY)
is incorrect. Checklist analysis uses historical information and information from similar projects within the organization's experience. Answer: A is incorrect. The Delphi technique uses rounds of anonymous surveys to generate a consensus on the identified risks. Answer: B is incorrect. Expert judgment is not the best answer for this; projects experts generally do the risk identification, in addition to the project team.

NEW QUESTION: 503
You are working in an enterprise. Your enterprise owned various risks. Which among the following is MOST likely to own the risk to an information system that supports a critical business process?

A. System users
B. Senior management
C. IT director
D. Risk management department
Answer: (SHOW ANSWER)
Section: Volume C
Explanation:
Senior management is responsible for the acceptance and mitigation of all risk. Hence they will also own the risk to an information system that supports a critical business process.
Incorrect Answers:
A: The system users are responsible for utilizing the system properly and following procedures, but they do not own the risk.
C: The IT director manages the IT systems on behalf of the business owners.
D: The risk management department determines and reports on level of risk, but does not own the risk. Risk is owned by senior management.

NEW QUESTION: 504
Which of the following sources is MOST relevant to reference when updating security awareness training materials?
A. Risk management framework
B. Recent security incidents reported by competitors
C. Global security standards
D. Risk register
Answer: (SHOW ANSWER)

NEW QUESTION: 505
Billy is the project manager of the HAR Project and is in month six of the project. The project is scheduled to last for 18 months.
Management asks Billy how often the project team is participating in risk reassessment in this project. What should Billy tell management if he's following the best practices for risk management?
A. Project risk management has been concluded with the project planning.
B. Project risk management happens at every milestone.
C. Project risk management is scheduled for every month in the 18-month project.
D. At every status meeting the project team project risk management is an agenda item.
E. Explanation:
Risk management is an ongoing project activity. It should be an agenda item at every project status meeting.
F. is incorrect. Milestones are good times to do reviews, but risk management should happen frequently.
G. is incorrect. This answer would only be correct if the project has a status meeting just

once per month in the project.
Answer: D,E,F,G (LEAVE A REPLY)
is incorrect. Risk management happens throughout the project as does project planning.

NEW QUESTION: 506
How are the potential choices of risk based decisions are represented in decision tree analysis?
A. End node
B. Root node
C. Event node
D. Decision node
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The potential choices of risk based decisions are represented in decision tree analysis via. Decision node, as decision nodes refers to the available choices.
Incorrect Answers:
A: End nodes are the final outcomes of the entire decision tree framework, especially in multilayered decision-making situations.
B: Root nodes represent the start of a decision tree.
C: Event nodes represents the possible uncertain outcomes of the decision, and not the available choices.

NEW QUESTION: 507
Which of the following would provide the BEST guidance when selecting an appropriate risk treatment plan?
A. Risk mitigation budget
B. Return on investment
C. Business Impact analysis
D. Cost-benefit analysis
Answer: (SHOW ANSWER)

NEW QUESTION: 508
An organization is considering modifying its system to enable acceptance of credit card payments. To reduce the risk of data exposure, which of the following should the organization do FIRST?
A. Implement additional controls
B. Conduct a risk assessment
C. Update the risk register
D. Update the security strategy
Answer: B (LEAVE A REPLY)
Section: Volume D

Explanation/Reference:

NEW QUESTION: 509
You are working as the project manager of the ABS project. The project is for establishing a computer network in a school premises. During the project execution, the school management asks to make the campus Wi-Fi enabled. You know that this may impact the project adversely. You have discussed the change request with other stakeholders. What will be your NEXT step?
A. Update project management plan.
B. Issue a change request.
C. Analyze the impact.
D. Update risk management plan.
E. Explanation:
The first step after receiving any change request in a project must be first analyzed for its impact. Changes may be requested by any stakeholder involved with the project. Although, they may be initiated verbally, they should always be recorded in written form and entered into the change management and/or configuration management.
Answer: C (LEAVE A REPLY)
B, and D are incorrect. All these are the required steps depending on the change request. Any change request must be followed by the impact analysis of the change.

NEW QUESTION: 510
You are working as a project manager in Bluewell Inc.. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?
A. Qualitative risk analysis
B. Risk audits
C. Quantitative risk analysis
D. Requested changes
E. Explanation:
Of all the choices given, only requested changes is an output of the monitor and control risks process. You might also have risk register updates, recommended corrective and preventive actions, organizational process assets, and updates to the project management plan.
F. and C are incorrect. These are the plan risk management processes.
Answer: D,E,F (LEAVE A REPLY)
is incorrect. Risk audit is a risk monitoring and control technique.

NEW QUESTION: 511
Which of the following components ensures that risks are examined for all new proposed change requests in the change control system?
A. Configuration management
B. Scope change control

C. Risk monitoring and control
D. Integrated change control
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
Integrated change control is the component that is responsible for reviewing all aspects of a change's impact on a project - including risks that may be introduced by the new change. Integrated change control is a way to manage the changes incurred during a project. It is a method that manages reviewing the suggestions for changes and utilizing the tools and techniques to evaluate whether the change should be approved or rejected. Integrated change control is a primary component of the project's change control system that examines the affect of a proposed change on the entire project.
Incorrect Answers:
A: Configuration management controls and documents changes to the features and functions of the product scope.
B: Scope change control focuses on the processes to allow changes to enter the project scope.
C: Risk monitoring and control is not part of the change control system, so this choice is not valid.

NEW QUESTION: 512
You are the project manager of the AFD project for your company. You are working with the project team to reassess existing risk events and to identify risk events that have not happened and whose relevancy to the project has passed. What should you do with these events that have not happened and would not happen now in the project?
A. Add the risk to the issues log
B. Close the outdated risks
C. Add the risks to the risk register
D. Add the risks to a low-priority watch-list
E. Explanation:
Risks that are now outdated should be closed by the project manager, there is no need to keep record of that.
F. is incorrect. Risks with low probability and low impact go on the risk watchlist.
G. is incorrect. Identified risks are already in the risk register.

Answer: B (LEAVE A REPLY)
is incorrect. Risks do not go into the issue log, but the risk register.

NEW QUESTION: 513
Which of the following is the MAIN reason for documenting the performance of controls?
A. Obtaining management sign-off
B. Providing accurate risk reporting
C. Demonstrating effective risk mitigation
D. Justifying return on investment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 514
Which of the following are external risk factors?
Each correct answer represents a complete solution. Choose three.
A. Geopolitical situation
B. Complexity of the enterprise
C. Market
D. Competition
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
These three are external risk factors as they lie outside the enterprise's control.
Incorrect Answers:
B: This includes geographic spread and value chain coverage (for example, in a manufacturing environment). That is why it is internal risk factor.

NEW QUESTION: 515
Which of the following represents a vulnerability?
A. Media recognition of an organization's market leadership in its industry
B. An identity thief seeking to acquire personal financial data from an organization
C. A standard procedure for applying software patches two weeks after release
D. An employee recently fired for insubordination
Answer: (SHOW ANSWER)

NEW QUESTION: 516
Which of the following is the MOST important consideration for a risk practitioner when making a system implementation go-live recommendation?
A. Results of end user acceptance testing
B. Variances between planned and actual cost
C. Completeness of system documentation
D. Availability of in-house resources

Answer: C (LEAVE A REPLY)

NEW QUESTION: 517
The MAIN purpose of having a documented risk profile is to:
A. enable well-informed decision making.
B. comply with external and internal requirements.
C. keep the risk register up-to-date.
D. prioritize investment projects.
Answer: A (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 518
An organization striving to be on the leading edge in regard to risk monitoring would MOST likely implement:
A. real-time monitoring of risk events and control exceptions.
B. a tool for monitoring critical activities and controls.
C. procedures to monitor the operation of controls.
D. monitoring activities for all critical assets.
Answer: (SHOW ANSWER)

NEW QUESTION: 519
You work as the project manager for Company Inc. The project on which you are working has several risks that will affect several stakeholder requirements. Which project management plan will define who will be available to share information on the project risks?
A. Resource Management Plan
B. Communications Management Plan
C. Risk Management Plan
D. Stakeholder management strategy
Answer: B (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The Communications Management Plan defines, in regard to risk management, who will be available to share information on risks and responses throughout the project.
The Communications Management Plan aims to define the communication necessities for the project and how the information will be circulated. The Communications Management Plan sets the communication structure for the project. This structure provides guidance for communication throughout the project's life and is updated as communication needs change. The Communication Managements Plan identifies and defines the roles of persons concerned with the project. It includes a matrix known as the communication matrix to map the communication requirements of the project.
Incorrect Answers:

A: The Resource Management Plan does not define risk communications.
C: The Risk Management Plan deals with risk identification, analysis, response, and monitoring.
D: The stakeholder management strategy does not address risk communications.

NEW QUESTION: 520
Which of the following is the BEST key control indicator (KCI) for a vulnerability management program?
A. Percentage of high-risk vulnerabilities missed
B. Defined thresholds for high-risk vulnerabilities
C. Percentage of high-risk vulnerabilities addressed
D. Number of high-risk vulnerabilities outstanding
Answer: C (LEAVE A REPLY)

NEW QUESTION: 521
What are the key control activities to be done to ensure business alignment?
Each correct answer represents a part of the solution. Choose two.
A. Define the business requirements for the management of data by IT
B. Conduct IT continuity tests on a regular basis or when there are major changes in the IT infrastructure
C. Periodically identify critical data that affect business operations
D. Establish an independent test task force that keeps track of all events
E. Explanation:
Business alignment require following control activities:
Defining the business requirements for the management of data by IT.
Periodically identifying critical data that affect business operations, in alignment with the risk management model and IT service as well as the business continuity plan.
F. is incorrect. Conducting IT continuity tests on a regular basis or when there are major changes in the IT infrastructure is done for testing IT continuity plan. It does not ensure alignment with business.
Answer: A,C (LEAVE A REPLY)
is incorrect. This is not valid answer.
TestsQuizNotesArticlesItemsReportsHelpBuy

NEW QUESTION: 522
A risk assessment has identified that departments have installed their own WiFi access points on the enterprise network. Which of the following would be MOST important to include in a report to senior management?
A. Planned remediation actions
B. The network security policy
C. The WiFi access point configuration
D. Potential business impact

Answer: (SHOW ANSWER)
Section: Volume D

NEW QUESTION: 523
You are the project manager of the NGQQ Project for your company. To help you communicate project status to your stakeholders, you are going to create a stakeholder register. All of the following information should be included in the stakeholder register except for which one?
A. Stakeholder management strategy
B. Assessment information of the stakeholders' major requirements, expectations, and potential influence
C. Identification information for each stakeholder
D. Stakeholder classification of their role in the project
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
The stakeholder management strategy is generally not included in the stakeholder registry because it may contain sensitive information that should not be shared with project team members or certain other individuals that could see the stakeholder register. The stakeholder register is a project management document that contains a list of the stakeholders associated with the project. It assesses how they are involved in the project and identifies what role they play in the organization. The information in this document can be very perceptive and is meant for limited exchange only. It also contains relevant information about the stakeholders, such as their requirements, expectations, and influence on the project.
Incorrect Answers:
B, C, D: Stakeholder identification, Assessment information, and Stakeholder classification should be included in the stakeholder register.

NEW QUESTION: 524
Which of the following are sub-categories of threat?
Each correct answer represents a complete solution. Choose three.
A. Natural and supernatural
B. Computer and user
C. Natural and man-made
D. Intentional and accidental
E. External and internal
Answer: C,D,E (LEAVE A REPLY)
Explanation/Reference:
Explanation:
A threat is any event which have the potential to cause a loss. In other word, it is any activity that represents a possible danger. The loss or danger is directly related to one of the following:

Loss of confidentiality- Someone sees a password or a company's secret formula, this is referred to as
- loss of confidentiality. Loss of integrity- An e-mail message is modified in transit, a virus infects a file, or someone makes unauthorized changes to a Web site is referred to as loss of integrity.
Loss of availability- An e-mail server is down and no one has e-mail access, or a file server is down so
- data files aren't available comes under loss of availability.

Threat identification is the process of creating a list of threats. This list attempts to identify all the possible threats to an organization. The list can be extensive.
Threats are often sub-categorized as under:
External or internal- External threats are outside the boundary of the organization. They can also be
- thought of as risks that are outside the control of the organization. While internal threats are within the boundary of the organization. They could be related to employees or other personnel who have access to company resources. Internal threats can be related to any hardware or software controlled by the business.

Natural or man-made- Natural threats are often related to weather such as hurricanes, tornadoes, and
- ice storms. Natural disasters like earthquakes and tsunamis are also natural threats. A human or man- made threat is any threat which is caused by a person. Any attempt to harm resources is a man-made threat. Fire could be man-made or natural depending on how the fire is started.

Intentional or accidental- An attempt to compromise confidentiality, integrity, or availability is intentional.
- While employee mistakes or user errors are accidental threats. A faulty application that corrupts data could also be considered accidental.

NEW QUESTION: 525
You are the project manager of HFD project. You have identified several project risks. You have adopted alternatives to deal with these risks which do not attempt to reduce the probability of a risk event or its impacts. Which of the following response have you implemented?
A. Acceptance
B. Mitigation
C. Avoidance
D. Contingent response
E. Explanation:
Contingent response strategy, also known as contingency planning, involves adopting alternatives to deal with the risks in case of their occurrence. Unlike the mitigation planning in which mitigation looks to reduce the probability of the risk and its impact, contingency planning

doesn't necessarily attempt to reduce the probability of a risk event or its impacts. Contingency comes into action when the risk event actually occurs.
F. is incorrect. Risk mitigation attempts to reduce the probability of a risk event and its impacts to an acceptable level. Risk mitigation can utilize various forms of control carefully integrated together. The main control types are:
Managerial(e.g.,policies)
Technical (e.g., tools such as firewalls and intrusion detection systems)
Operational (e.g., procedures, separation of duties)
Preparedness activities
G. is incorrect. Risk acceptance means that no action is taken relative to a particular risk; loss is accepted if it occurs. If an enterprise adopts a risk acceptance, it should carefully consider who can accept the risk. Risk should be accepted only by senior management in relationship with senior management and the board. There are two alternatives to the acceptance strategy, passive
and active.
Passive acceptance means that enterprise has made no plan to avoid or mitigate the risk but willing to accept the consequences of the risk.
Active acceptance is the second strategy and might include developing contingency plans and reserves to deal with risks.
Answer: D,E,F,G (LEAVE A REPLY)
is incorrect. Risk avoidance means to evade risk altogether, eliminate the cause of the risk event, or change the project plan to protect the project objectives from the risk event.

NEW QUESTION: 526
An organization has outsourced its billing function to an external service provider. Who should own the risk of customer data leakage caused by the service provider?
A. The service provider
B. Business process owner
C. Vendor risk manager
D. Legal counsel
Answer: B (LEAVE A REPLY)
Section: Volume D

NEW QUESTION: 527
A third-party vendor has offered to perform user access provisioning and termination. Which of the following control accountabilities is BEST retained within the organization?
A. Reviewing access control lists
B. Terminating inactive user access
C. Performing user access recertification
D. Authorizing user access requests
Answer: D (LEAVE A REPLY)