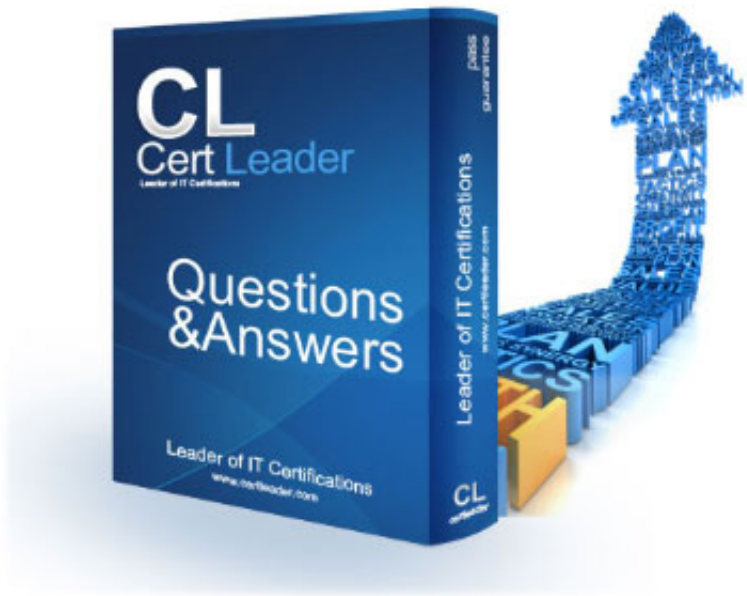
CRISC - Certified in Risk and Information Systems Control

http://www.certleader.com/CRISC-dumps.html



1.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

Answer: D

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:** B 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.

2.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: C

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.**Answer:** D is incorrect.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.**Answer:** A is incorrect.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.**Answer:** B is incorrect.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.

3.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.

Answer: D

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:** B 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.

4.You are the project manager of a large construction project.This project will last for 18 months and will cost $750,000 to complete.You are working with your project team, experts, and stakeholders to identify risks within the project before the project work begins.Management wants to know why you have scheduled so many risk identification meetings throughout the project rather than just initially during the project planning.What is the best reason for the duplicate risk identification sessions?

A.The iterative meetings allow all stakeholders to participate in the risk identification processes throughout the project phases.

B.The iterative meetings allow the project manager to discuss the risk events which have passed the project and which did not happen.

C.The iterative meetings allow the project manager and the risk identification participants to identify newly discovered risk events throughout the project.

D.The iterative meetings allow the project manager to communicate pending risks events during project execution.

Answer: C

Explanation:

Risk identification is an iterative process because new risks may evolve or become known as the project progresses through its life cycle.**Answer:** D is incorrect.The primary reason for iterations of risk identification is to identify new risk events.**Answer:** B is incorrect.Risk identification focuses on discovering

new risk events, not the events which did not happen.**Answer:** A is incorrect.Stakeholders are encouraged to participate in the risk identification process, but this is not the best choice for the

5.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: A

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 **Answer:** C, D, and B are incorrect.These are not RPN for given values of severity, occurrence, and detection.

6.Which of the following is the MOST important use of KRIs?

A.Providing a backward-looking view on risk events that have occurred

B.Providing an early warning signal

C.Providing an indication of the enterprise\'s risk appetite and tolerance

D.Enabling the documentation and analysis of trends

Answer: B

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.As KRIs are the indicators of risk, hence its most important function is to effectively give an early warning signal that a high risk is emerging to enable management to take proactive action before the risk actually becomes a loss.**Answer:** D is incorrect.This is not as important as giving early warning.**Answer:** A is incorrect.This is one of the important functions of KRIs which can help management

to improve but is not as important as giving early warning.**Answer:** C is incorrect.KRIs provide an indication of the enterprise\'s risk appetite and tolerance through metric setting, but this is not as important as giving early warning.

7.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

Answer: A,B

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:** D and C are incorrect.Chief financial officer and human resource only overview common risk view, but are not involved in risk based decisions.

8.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: B,C,D

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.**Answer:** A is incorrect.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.

9.You work as the project manager for Bluewell Inc.Your project 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.Risk Management Plan

C.Stakeholder management strategy

D.Communications Management Plan

Answer: D

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 forcommunication 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:** C is incorrect.The stakeholder management strategy does not address risk communications.**Answer:** B is incorrect.The Risk Management Plan defines risk identification, analysis, response, and monitoring.**Answer:** A is incorrect.The Resource Management Plan does not define risk communications.

10.Which of the following controls is an example of non-technical controls?

A.Access control

B.Physical security

C.Intrusion detection system

D.Encryption

Answer: B

Explanation:

Physical security is an example of non-technical control.It comes under the family of operational controls.**Answer:** C, A, and D are incorrect.Intrusion detection system, access control, and encryption are the safeguards that are incorporated into computer hardware, software or firmware, hence they refer to as technical controls.

11.You are the project manager of GHT project.Your project team is in the process of identifying project risks on your current project.The team has the option to use all of the following tools and techniques to diagram some of these potential risks EXCEPT for which one?

A.Process flowchart

B.Ishikawa diagram

C.Influence diagram

D.Decision tree diagram

Answer: D

Explanation:

Decision tree diagrams are used during the Quantitative risk analysis process and not in risk identification.**Answer:** B, A, and C are incorrect.All the these options are diagrammatical techniques used in the Identify risks process.

12.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

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.**Answer:** C is incorrect.It is not the valid definition.**Answer:** A is incorrect.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.**Answer:** B is incorrect.It is not the valid definition.

13.Which of the following aspect of monitoring tool ensures that the monitoring tool has the ability to keep up with the growth of an enterprise?

A.Scalability

B.Customizability

C.Sustainability

D.Impact on performance

Answer: A

Explanation:

Monitoring tools have to be able to keep up with the growth of an enterprise and meet anticipated growth in process, complexity or transaction volumes; this is ensured by the scalability criteria of the monitoring tool.**Answer:** C is incorrect.It ensures that monitoring software is able to change at the same speed as technology applications and infrastructure to be effective over time.**Answer:** B is incorrect.For software to be effective, it must be customizable to the specific needs of an enterprise.Hence customizability ensures that end users can adapt the software.**Answer:** D is incorrect.The impact on performance has nothing related to the ability of monitoring tool to keep up with the growth of enterprise.

14.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

Explanation:

Moderate risks are noticeable failure threatening the success of certain goals.**Answer:** C is incorrect.Extremely high risk are the risks that has large impact on enterprise and are most likely results in failure with severe consequences.**Answer:** B is incorrect.High risk is the significant failure impacting in certain goals not being met.**Answer:** D is incorrect.Low risks are the risk that results in certain unsuccessful goals.

15.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

Explanation:

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.

16.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.Risk identification

C.Risk response planning

D.Risk communication

Answer: D

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.**Answer:** C is incorrect.A risk response ensures that the residual risk is within the limits of the risk appetite and tolerance of the enterprise.Risk response is process of selecting the correct, prioritized response to risk, based on the level of risk, the enterprise\'s risk tolerance and the cost and benefit of the particular risk

response option.Risk response ensures that management is providing accurate reports on: The level of risk faced by the enterprise The incidents\' type that have occurred Any alteration in the enterprise\'s risk profile based on changes in the risk environment

17.You are an experienced Project Manager that has been entrusted with a project to develop a machine which produces auto components.You have scheduled meetings with the project team and the key stakeholders to identify the risks for your project.Which of the following is a key output of this process?

A.Risk Register

B.Risk Management Plan

C.Risk Breakdown Structure

D.Risk Categories

Answer: A

Explanation:

The primary outputs from Identify Risks are the initial entries into the risk register.The risk register ultimately contains the outcomes of other risk management processes as they are conducted, resulting in an increase in the level and type of information contained in the risk register over time.**Answer:** B, D, and C are incorrect.All these are outputs from the "Plan Risk Management" process, which happens prior to the starting of risk identification.

18.Which of the following components of risk scenarios has the potential to generate internal or external threat on an enterprise?

A.Timing dimension

B.Events

C.Assets

D.Actors

Answer: D

Explanation:

Components of risk scenario that are needed for its analysis are: Actor: Actors are those components of risk scenario that has the potential to generate the threat that can be internal or external, human or non-human.Internal actors are within the enterprise like staff, contractors, etc.On the other hand, external actors include outsiders, competitors, regulators and the market.Threat type: Threat type defines the nature of threat, that is, whether the threat is malicious, accidental, natural or intentional.Event: Event is an essential part of a scenario; a scenario always has to contain an event.Event describes the happenings like whether it is a disclosure of confidential information, or interruption of a system or project, or modification, theft, destruction, etc.Asset: 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.Timing dimension: The timing dimension is the application of the scenario to detect time to respond to or recover from an event.It identifies if the event occur at a critical moment and its duration.It also specifies the time lag between the event and the consequence, that is, if there an immediate consequence (e.g., network failure, immediate downtime) or a delayed consequence (e.g., wrong IT architecture with accumulated high costs over a long period of time).

19.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: A,C

Explanation:

Pilot testing and reviewing of performance data to verify operation against design are done before relying on control.**Answer:** D is incorrect.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.**Answer:** B is incorrect.Discovering risk exposure helps in identifying the severity of risk, but it does not play any role in specifying the reliability of control.

20.Which of the following is NOT true for risk management capability maturity level 1?

A.There is an understanding that risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk

B.Decisions involving risk lack credible information

C.Risk appetite and tolerance are applied only during episodic risk assessments

D.Risk management skills exist on an ad hoc basis, but are not actively developed

Answer: B

Explanation:

The enterprise with risk management capability maturity level 0 makes decisions without having much knowledge about the risk credible information.In level 1, enterprise takes decisions on the basis of risk credible information.**Answer:** A, C, and D are incorrect.An enterprise\'s risk management capability maturity level is 1 when: There is an understanding that risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk.Any risk identification criteria vary widely across the enterprise.Risk appetite and tolerance are applied only during episodic risk assessments.Enterprise risk policies and standards are incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms.Risk management

skills exist on an ad hoc basis, but are not actively developed.

Ad hoc inventories of controls that are unrelated to risk are dispersed across desktop applications.

21.An enterprise has identified risk events in a project.While responding to these identified risk events, which among the following stakeholders is MOST important for reviewing risk response options to an IT risk.

A.Information security managers

B.Internal auditors

C.Incident response team members

D.Business managers

Answer: D

Explanation:

Business managers are accountable for managing the associated risk and will determine what actions to take based on the information provided by others.**Answer:** A is incorrect.Information security managers may best understand the technical tactical situation, but business managers are accountable for managing the associated risk and will determine what actions to take based on the information provided by others, which includes collaboration with, and support from, IT security managers.**Answer:** C is incorrect.The incident response team must ensure open communication to management and stakeholders to ensure that business managers understand the associatedrisk and are provided enough information to make informed risk-based decisions.They are not responsible for reviewing risk response options.

22.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

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.**Answer:** B is incorrect.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.**Answer:** D is incorrect.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.**Answer:** A is incorrect.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

23.What is the process for selecting and implementing measures to impact risk called?

A.Risk Treatment

B.Control

C.Risk Assessment

D.Risk Management

Answer: A

Explanation:

The process for selecting and implementing measures for impacting risk in the environment is called risk treatment.**Answer:** A is incorrect.Risk management is the coordinated activities for directing and controlling the treatment of risk in the organization.**Answer:** C is incorrect.The process of analyzing and

evaluating risk is called risk assessment.

24.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

Explanation:

Section 302 of the Sarbanes-Oxley Act requires corporate responsibility for financial reports to be certified by CEO, CFO, or designated representative.**Answer:** C is incorrect.Section 203 of the Sarbanes-Oxley Act requires audit partners and review partners to rotate off an assignment every five years.**Answer:** D is incorrect.Section 409 of the Sarbanes-Oxley Act states that the financial reports must be distributed quickly and currently.**Answer:** B is incorrect.Section 404 of the Sarbanes-Oxley Act states that annual assessments of internal controls are the responsibility of management.

25.What is the PRIMARY need for effectively assessing controls?

A.Control\'s alignment with operating environment

B.Control\'s design effectiveness

C.Control\'s objective achievement

D.Control\'s operating effectiveness

Answer: C

Explanation:

Controls can be effectively assessed only by determining how accurately the control objective is achieved within the environment in which they are operating.No conclusion can be reached as to the strength of the

control until the control has been adequately tested.**Answer:** B is incorrect.Control\'s design effectiveness is also considered but is latter considered after achieving objectives.**Answer:** D is incorrect.Control\'s operating effectiveness is considered but after its accuracy in objective achievement.**Answer:** A is incorrect.Alignment of control with the operating environment is essential but after the control\'s accuracy in achieving objective.In other words, achieving objective is the top most priority in assessing controls.

26.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

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

27.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: B

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.**Answer:** C is incorrect.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.**Answer:** A is incorrect.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.**Answer:** D is incorrect.David has not hired a vendor to manage the risk for his project; therefore he is not transferring the risk.

28.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: 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.**Answer:** B, D, and C are incorrect.These are also the objectives of the information system control but are not the best answer.

29.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

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.**Answer:** C is incorrect.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.**Answer:** B is incorrect.Index of Disaster-Relevant Information is a catalogue 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.**Answer:** D is incorrect.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.

30.For which of the following risk management capability maturity levels do the statement given below is true? "Real-time monitoring of risk events and control exceptions exists, as does automation of policy management"

A.Level 3

B.Level 0

C.Level 5

D.Level 2

Answer: C

Explanation:

An enterprise\'s risk management capability maturity level is 5 when real-time monitoring of risk events and control exceptions exists, as does automation of policy management.**Answer:** B is incorrect.In level 0 of risk management capability maturity model, enterprise does

not recognize the importance of considering the risk management or the business impact from IT risk.**Answer:** A and D are incorrect.In these levels real-time monitoring of risk events is not done.

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your CRISC Exam with Our Prep Materials Via below:

http://www.certleader.com/CRISC-dumps.html