Pass4sure CAP 276q

Number: CAP
Passing Score: 800
Time Limit: 120 min
File Version: 16.5

ISC CAP

CAP Certified Authorization Professional

Passed on 2-02-15 with an 890. Dump still valid in US. 1 or 2 new questions. You must know the material as answers are worded differently at times.

Exam A

QUESTION 1
Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process?

A. Senior Agency Information Security Officer
B. Authorizing Official
C. Common Control Provider
D. Chief Information Officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

Each correct answer represents a complete solution. Choose all that apply.

A. Preserving high-level communications and working group relationships in an organization
B. Facilitating the sharing of security risk-related information among authorizing officials
C. Establishing effective continuous monitoring program for the organization
D. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

A. Information system owner
B. Authorizing Official

C. Chief Risk Officer (CRO)
D. Chief Information Officer (CIO)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 4
Which of the following assessment methodologies defines a six-step technical security evaluation?

A. FITSAF
B. FIPS 102
C. OCTAVE
D. DITSCAP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 5
DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. What phases are identified by DIACAP?

Each correct answer represents a complete solution. Choose all that apply.

Real 3
ISC CAP Exam

A. Accreditation
B. Identification
C. System Definition
D. Verification
E. Validation
F. Re-Accreditation

Correct Answer: CDEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 6
James work as an IT systems personnel in SoftTech Inc. He performs the following tasks:

Runs regular backups and routine tests of the validity of the backup data.

Real 4
ISC CAP Exam
Performs data restoration from the backups whenever required.

Maintains the retained records in accordance with the established information classification policy.

What is the role played by James in the organization?

A. Manager
B. Owner
C. Custodian
D. User

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 7
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 4
B. Level 1
C. Level 3
D. Level 5

E. Level 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 8
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation?

Each correct answer represents a complete solution. Choose two.

A. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
C. Certification is the official management decision given by a senior agency official to authorize operation of an information system.
D. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 9
Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production?

Each correct answer represents a part of the solution. Choose all that apply.

Real 6
ISC CAP Exam

A. NIST
B. FIPS
C. FISMA
D. Office of Management and Budget (OMB)

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 10
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP accreditation?

Each correct answer represents a complete solution. Choose all that apply.

A. Secure accreditation
B. Type accreditation
C. System accreditation
D. Site accreditation

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information

Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD?

Each correct answer represents a complete solution. Choose all that apply.

A. VI Vulnerability and Incident Management
B. DC Security Design & Configuration
C. EC Enclave and Computing Environment
D. Information systems acquisition, development, and maintenance

Correct Answer: ABC
Section: (none)

Explanation

Explanation/Reference:
Explanation:

Real 7
ISC CAP Exam

QUESTION 12
Ben is the project manager of the YHT Project for his company. Alice, one of his team members, is confused about when project risks will happen in the project. Which one of the following statements is the most accurate about when project risk happens?

A. Project risk can happen at any moment.
B. Project risk is uncertain, so no one can predict when the event will happen.
C. Project risk happens throughout the project execution.
D. Project riskis always in the future.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Real 8
ISC CAP Exam

Explanation:

QUESTION 13
You are the project manager of the NKJ Project for your company. The project's success or failure will have a significant impact on your organization's profitability for the coming year. Management has asked you to identify the risk events and communicate the event's probability and impact as early as possible in the project. Management wants to avoid risk events and needs to analyze the cost-benefits of each risk event in this project. What term is assigned to the low-level of stakeholder tolerance in this project?

A. Risk avoidance
B. Mitigation-ready project management
C. Risk utility function
D. Risk-reward mentality

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 14
There are five inputs to the quantitative risk analysis process. Which one of the following is NOT an input to the perform quantitative risk analysis process?

A. Risk register
B. Cost management plan
C. Risk management plan
D. Enterprise environmental factors
Real 9
ISC CAP Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
Your project has several risks that may cause serious financial impact should they happen. You have studied the risk events and made some potential risk responses for the risk events but management wants you to do more. They'd like for you to create some type of a chart that identified the risk probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

A. Risk response plan
B. Quantitative analysis
C. Risk response
D. Contingency reserve

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 16
You are working as a project manager in your organization. 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. Quantitative risk analysis
B. Qualitative risk analysis
Real 10
ISC CAP Exam
C. Requested changes
D. Risk audits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
The phase 3 of the Risk Management Framework (RMF) process is known as mitigation planning.

Which of the following processes take place in phase 3?

Each correct answer represents a complete solution. Choose all that apply.

A. Identify threats, vulnerabilities, and controls that will be evaluated.
B. Document and implement a mitigation plan.
C. Agree on a strategy to mitigate risks.
D. Evaluate mitigation progress and plan next assessment.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 18
Gary is the project manager of his organization. He is managing a project that is similar to a project his organization completed recently. Gary has decided that he will use the information from the past project to help him and the project team to identify the risks that may be present in the project. Management agrees that this checklist approach is ideal and will save time in the project.

Real 11

ISC CAP Exam
Which of the following statement is most accurate about the limitations of the checklist analysis approach for Gary?

A. The checklist analysis approach is fast but it is impossible to build and exhaustive checklist.
B. The checklist analysis approach only uses qualitative analysis.
C. The checklist analysis approach saves time, but can cost more.
D. The checklist is also known as top down risk assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 19
Information risk management (IRM) is the process of identifying and assessing risk, reducing it to an acceptable level, and implementing the right mechanisms to maintain that level. What are the different categories of risk?

Each correct answer represents a complete solution. Choose all that apply.

A. System interaction
B. Human interaction
C. Equipment malfunction
D. Inside and outside attacks
E. Social status
F. Physical damage

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: B,C,D,E,F

Real 12
ISC CAP Exam

Explanation:

QUESTION 20

In which type of access control do user ID and password system come under?

A. Administrative
B. Technical
C. Power
D. Physical

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 21
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 accepted.
B. These risks can be added to a low priority risk watch list.
C. All risks must have a valid, documented risk response.
D. These risks can be dismissed.
Real 13
ISC CAP Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 22
Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe.

What type of risk response has Adrian used in this example?

A. Mitigation
B. Transference

C. Avoidance
D. Acceptance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 23
Which of the following is an entry in an object's discretionary access control list (DACL) that grants permissions to a user or group?

A. Access control entry (ACE)
B. Discretionary access control entry (DACE)
C. Access control list (ACL)
D. Security Identifier (SID)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 24
You are the project manager for your organization. You have identified a risk event you're your organization could manage internally or externally. If you manage the event internally it will cost your project $578,000 and an additional $12,000 per month the solution is in use. A vendor can manage the risk event for you. The vendor will charge $550,000 and $14,500 per month that the solution is in use. How many months will you need to use the solution to pay for the internal solution in comparison to the vendor's solution?

A. Approximately 13 months
B. Approximately 11 months
C. Approximately 15 months
D. Approximately 8 months

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 15
ISC CAP Exam

QUESTION 25
Management wants you to create a visual diagram of what resources will be utilized in the project deliverables. What type of a chart is management asking you to create?

A. Work breakdown structure
B. Resource breakdown structure
C. RACI chart
D. Roles and responsibility matrix

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
You are preparing to start the qualitative risk analysis process for your project. You will be relying on some organizational process assets to influence the process. Which one of the following is NOT a probable reason for relying on organizational process assets as an input for qualitative risk analysis?

A. Information on prior, similar projects
B. Review of vendor contracts to examine risks in past projects
C. Risk databases that may be available from industry sources
D. Studies of similar projects by risk specialists

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 16
ISC CAP Exam

QUESTION 27
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?

A. Avoidance
B. Mitigation
C. Exploit
D. Transference

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test?

Each correct answer represents a complete solution. Choose all that apply.

A. Social engineering
B. File and directory permissions
C. Buffer overflows
D. Kernel flaws
E. Race conditions
F. Information system architectures
G. Trojan horses

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: A,B,C,D,E,G
Explanation:

QUESTION 29
Frank is the project manager of the NHH Project. He is 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 is Frank and the NHH Project team creating in this scenario?

A. Project management plan
B. Resource management plan
C. Risk management plan
D. Project plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

A. Phase 4
B. Phase 3
C. Phase 2
D. Phase 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 31
Which of the following roles is also known as the accreditor?

A. Chief Risk Officer
B. Data owner
C. Designated Approving Authority
D. Chief Information Officer
Real 19
ISC CAP Exam

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 32
In which of the following phases of the DITSCAP process does Security Test and Evaluation (ST&E) occur?

A. Phase 2
B. Phase 3
C. Phase 1
D. Phase 4

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 33
You are the project manager of the NHH project for your company. You have completed the first round of risk management planning and have created four outputs of the risk response planning process. Which one of the following is NOT an output of the risk response planning?

A. Risk-related contract decisions
B. Project document updates
C. Risk register updates
D. Organizational process assets updates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 34
You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NHH Project has a budget at completion of $945,000 and is 45 percent complete though the project should be 49 percent

complete. The project has spent $455,897 to reach the 45 percent complete milestone.

What is the project's schedule performance index?

A. 1.06
B. 0.92
C. -$37,800
D. 0.93

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 35
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

Real 21
ISC CAP Exam

A. Security law
B. Privacy law
C. Copyright law
D. Trademark law

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 36
Which of the following is a 1996 United States federal law, designed to improve the way the federal government acquires, uses, and disposes information technology?

A. Computer Misuse Act
B. Lanham Act

C. Clinger-CohenAct
D. Paperwork Reduction Act

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 37
Which of the following is used to indicate that the software has met a defined quality level and is

Real 22
ISC CAP Exam
ready for mass distribution either by electronic means or by physical media?

A. RTM
B. CRO
C. DAA
D. ATM

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 38
Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

A. Procurement management
B. Change management
C. Risk management
D. Configuration management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 23
ISC CAP Exam

QUESTION 39
Which of the following RMF phases is known as risk analysis?

A. Phase 2
B. Phase 1
C. Phase 0
D. Phase 3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 40
Jenny is the project manager of the NHJ Project for her company. She has identified several positive risk events within the project and she thinks these events can save the project time and money. You, a new team member wants to know that how many risk responses are available for a positive risk event. What will Jenny reply to you?

A. Four
B. Seven
C. Acceptance is the only risk response for positive risk events.
D. Three

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 24
ISC CAP Exam

QUESTION 41
You are the project manager for the NHH project. You are working with your project team to examine the project from four different defined perspectives to increase the breadth of identified risks by including internally generated risks. What risk identification approach are you using in this example?

A. SWOT analysis
B. Root cause analysis
C. Assumptions analysis
D. Influence diagramming techniques

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 25
ISC CAP Exam

QUESTION 42
Which of the following are included in Physical Controls?

Each correct answer represents a complete solution. Choose all that apply.

A. Locking systems and removing unnecessary floppy or CD-ROM drives
B. Environmental controls
C. Password and resource management
D. Identification and authentication methods
E. Monitoring for intrusion
F. Controlling individual access into the facilityand different departments

Correct Answer: ABEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 43
Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-60
B. NIST SP 800-53A
C. NIST SP 800-37
D. NIST SP 800-42
E. NIST SP 800-59
F. NIST SP 800-53

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 44
You are the project manager of the GHG project. You are preparing for the quantitative risk analysis process. You are using organizational process assets to help you complete the quantitative risk analysis process. Which one of the following is NOT a valid reason to utilize organizational process assets as a part of the quantitative risk analysis process?

A. You will use organizational process assets for risk databases that may be available from industry sources.
B. You will use organizational process assets for studies of similar projects by risk specialists.
C. You will use organizational process assets to determine costs of all risks events within thecurrent project.
D. You will use organizational process assets for information from prior similar projects.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 45
You and your project team are just starting the risk identification activities for a project that is scheduled to last for 18 months. Your project team has already identified a long list of risks that need to be analyzed. How often should you and the project team do risk identification?

A. At least once per month
B. Identify risks is an iterative process.
C. It depends on how many risks are initially identified.
D. Several times until the project moves into execution

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 46
Eric is the project manager of the MTC project for his company. In this project a vendor has offered Eric a sizeable discount on all hardware if his order total for the project is more than $125,000. Right now, Eric is likely to spend $118,000 with vendor. If Eric spends $7,000 his cost savings for the project will be $12,500, but he cannot purchase hardware if he cannot implement the hardware immediately due to organizational policies. Eric consults with Amy and Allen, other project managers in the organization, and asks if she needs any hardware for their projects. Both Amy and Allen need hardware and they agree to purchase the hardware through Eric's relationship with the vendor. What positive risk response has happened in this instance?

A. Transference
B. Exploiting
C. Sharing
D. Enhancing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 47
You work as a project manager for BlueWell Inc. You are preparing to plan risk responses for your project with your team. How many risk response types are available for a negative risk event in the project?

A. Seven
B. Three
C. Four
D. One

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 48
You are the project manager for a construction project. The project includes a work that involves very high financial risks. You decide to insure processes so that any ill happening can be compensated. Which type of strategies have you used to deal with the risks involved with that particular work?

A. Transfer
B. Mitigate
C. Accept
Real 29
ISC CAP Exam
D. Avoid

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 49
Which of the following are included in Administrative Controls?

Each correct answer represents a complete solution. Choose all that apply.

A. Conducting security-awareness training
B. Screening of personnel
C. Monitoring for intrusion
D. Implementing change control procedures
E. Developing policy

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 50
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. What are the process activities of this phase?

Each correct answer represents a complete solution. Choose all that apply.

A. Configuring refinement of the SSAA
B. Assessment of the Analysis Results
C. System development
D. Certification analysis
E. Registration

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 51
You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software

Real 30
ISC CAP Exam
you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?

A. Sharing
B. Avoidance
C. Transference
D. Exploiting

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 52

Which of the following are the common roles with regard to data in an information classification program?

Each correct answer represents a complete solution. Choose all that apply.

A. Custodian
B. User
C. Security auditor
D. Editor
E. Owner

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 53
To help review or design security controls, they can be classified by several criteria. One of these criteria is based on nature. According to this criteria, which of the following controls consists of incident response processes, management oversight, security awareness, and training?

A. Technical control
B. Physical control
C. Procedural control
D. Compliance control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 54
An Authorizing Official plays the role of an approver. What are the responsibilities of an

Authorizing Official?

Each correct answer represents a complete solution. Choose all that apply.

A. Establishing and implementing the organization's continuous monitoring program

B. Determining the requirement of reauthorization and reauthorizing information systems when required

C. Reviewing security status reports and critical security documents

D. Ascertaining the security posture of the organization's information system Real 32
ISC CAP Exam

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 55
You work as a project manager for SoftTech Inc. You are working with the project stakeholders to begin the qualitative risk analysis process. You will need all of the following as inputs to the qualitative risk analysis process except for which one?

A. Risk management plan

B. Risk register

C. Stakeholder register

D. Project scope statement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 56
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Configuration Management System

B. Project Management InformationSystem

C. Scope Verification

D. Integrated Change Control
Real 33
ISC CAP Exam

Correct Answer: A
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 57
Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

A. Chief Information Security Officer
B. Senior Management
C. Information Security Steering Committee
Real 34
ISC CAP Exam
D. Business Unit Manager

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 58
Your organization has a project that is expected to last 20 months but the customer would really like the project completed in 18 months. You have worked on similar projects in the past and believe that you could fast track the project and reach the 18 month deadline. What increases when you fast track a project?

A. Risks
B. Costs
C. Resources
D. Communication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 59
The IAM/CA makes certification accreditation recommendations to the DAA. The DAA issues accreditation determinations. Which of the following are

the accreditation determinations issued by the DAA?

Each correct answer represents a complete solution. Choose all that apply.

A. IATO
B. ATO
C. IATT
D. ATT
E. DATO

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 60
You are the project manager of the NKQ project for your organization. You have completed the quantitative risk analysis process for this portion of the project. What is the only output of the quantitative risk analysis process?

A. Probability of reaching project objectives
B. Risk contingency reserve
C. Risk response
D. Risk register updates

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 61
You work as the project manager for Bluewell Inc. You are working on NGQQ Projectyou're your

Real 36
ISC CAP Exam
company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

A. Risk acceptance
B. Risk avoidance
C. Risk transference
D. Risk mitigation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 62
You work as a project manager for BlueWell Inc. You are currently working with the project stakeholders to identify risks in your project. You understand that the qualitative risk assessment and analysis can reflect the attitude of the project team and other stakeholders to risk. Effective assessment of risk requires management of the risk attitudes of the participants. What should you, the project manager, do with assessment of identified risks in consideration of the attitude and bias of the participants towards the project risk?

A. Document the bias for the risk events and communicate the bias with management
B. Evaluate and document the bias towards the risk events
C. Evaluate the bias through SWOT for true analysis of the risk events
D. Evaluate the bias towards the risk events and correct the assessment accordingly

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 63
Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

A. Circumstantial
B. Incontrovertible
C. Direct
D. Corroborating

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 37
ISC CAP Exam

Topic 2, Volume B

QUESTION 64
You work as a project manager for BlueWell Inc. You are working with Nancy, the COO of your company, on several risks within the project. Nancy understands that through qualitative analysis you have identified 80 risks that have a low probability and low impact as the project is currently planned. Nancy's concern, however, is that the impact and probability of these risk events may change as conditions within the project may change. She would like to know where will you document and record these 80 risks that have low probability and low impact for future reference.

What should you tell Nancy?

A. Risk identification is an iterative process so any changes to the low probability and low impact risks will be reassessed throughout the project life cycle.
B. Risks with low probability and low impact are recorded in a watchlist for future monitoring.
C. All risks, regardless of their assessed impact and probability, are recorded in the risk log.
D. All risks are recorded in the risk management plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 65
You work as a project manager for BlueWell Inc. Management has asked you to work with the key

Real 38
ISC CAP Exam
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 the 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. Focus on the high-priority risks through qualitative risk analysis
C. Use qualitative risk analysis to quickly assess the probability and impact of risk events
D. Involve the stakeholders for risk identification only in the phases where the project directlyaffects them

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 66
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 profityou're your organization seizes this opportunity it would be an example of what risk response?

A. Opportunistic
B. Positive
C. Enhancing
D. Exploiting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 67
Which of the following NIST documents provides a guideline for identifying an information system as a National Security System?

A. NIST SP 800-53
B. NIST SP 800-59
C. NIST SP 800-53A
D. NIST SP 800-37
E. NIST SP 800-60

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 68
There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

A. Acceptance
B. Mitigation
C. Sharing
D. Transference

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Real 40
ISC CAP Exam

Explanation:

QUESTION 69
What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

A. PON
B. ZOPA
C. BATNA
D. Bias

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 70
Which of the following is the acronym of RTM?

A. Resource tracking method
B. Requirements Traceability Matrix
C. Resource timing method
D. Requirements Testing Matrix

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 71
Which of the following are the tasks performed by the owner in the information classification schemes?

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

A. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
B. To perform data restoration from the backups whenever required.
C. To review the classification assignments from time to time and make alterations as the business requirements alter.
D. To delegate the responsibility of the data safeguard duties to the custodian.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 72
Which of the following approaches can be used to build a security program?

Each correct answer represents a complete solution. Choose all that apply.

A. Bottom-Up Approach
B. Right-Up Approach
C. Top-Down Approach
D. Left-Up Approach

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Real 42
ISC CAP Exam

Explanation:

QUESTION 73
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 organizations can create risk scores for each objective of the project.
B. Harry is correct, because the risk probability and impact considers all objectives of the project.
C. Harry is correct, the risk probability and impact matrix is the only approach to risk assessment.
D. Sammy is correct, because she is the project manager.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 74
Which of the following phases of the DITSCAP C&A process is used to define the C&A level of effort, to identify the main C&A roles and responsibilities, and to create an agreement on the method for implementing the security requirements?

Real 43
ISC CAP Exam

A. Phase 3
B. Phase 2
C. Phase 4
D. Phase 1

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 75
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy?

Each correct answer represents a part of the solution. Choose all that apply.

A. Who is expected to exploit the vulnerability?
B. What is being secured?
C. Where is the vulnerability, threat, or risk?
D. Who is expected to comply with the policy?

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 76
Which of the following objectives are defined by integrity in the C.I.A triad of information security systems?

Real 44
ISC CAP Exam
Each correct answer represents a part of the solution. Choose three.

A. It preserves the internal and external consistency of information.
B. It prevents the unauthorized or unintentional modification of information by the authorized users.
C. It prevents the intentional or unintentional unauthorized disclosure of a message's contents .
D. It prevents the modification of information by the unauthorized users.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 77
Which of the following are the goals of risk management?

Each correct answer represents a complete solution. Choose three.

A. Finding an economic balance between the impact of the risk and the cost of the countermeasure
B. Identifying the risk
C. Assessing the impact of potential threats
D. Identifying the accused

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 78
Real 45
ISC CAP Exam
You are the project manager of the GHG project. You are preparing for the quantitative risk analysis process. You are using organizational process assets to help you complete the quantitative risk analysis process. Which one of the following is NOT a valid reason to utilize organizational process assets as a part of the quantitative risk analysis process?

A. You will use organizational process assets for studies of similar projects by risk specialists.
B. You will use organizational process assets to determine costs of all risks events within the current project.
C. You will use organizational process assets for information from prior similar projects.
D. You will use organizational process assets for risk databases that may be available from industry sources.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 79
Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

A. SSAA
B. FIPS
C. FITSAF
D. TCSEC

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 80
Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

A. Acceptance
B. Mitigation
C. Avoidance
D. Transference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Real 46
ISC CAP Exam

Explanation:

QUESTION 81
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. Risk register

B. Risk management plan
C. Project charter
D. Quality management plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 82
Mary is the project manager of the HGH Project for her company. She and her project team have agreed that if the vendor is late by more than ten days they will cancel the order and hire the NBG Company to fulfill the order. The NBG Company can guarantee orders within three days, but the costs of their products are significantly more expensive than the current vendor. What type of a response strategy is this?

A. External risk response
B. Internal risk management strategy
C. Contingent response strategy
D. Expert judgment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 83
Your project uses a piece of equipment that if the temperature of the machine goes above 450 degree Fahrenheit the machine will overheat and have to be shut down for 48 hours. Should this machine overheat even once it will delay the project's end date. You work with your project to create a response that should the temperature of the machine reach 430, the machine will be paused for at least an hour to cool it down. The temperature of 430 is called what?

A. Risk identification
B. Risk response
Real 48
ISC CAP Exam
C. Risk trigger
D. Risk event

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 84
According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information

Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD?

Each correct answer represents a complete solution. Choose all that apply.

A. DC Security Design & Configuration
B. VI Vulnerability and Incident Management
C. EC Enclave and Computing Environment
D. Information systems acquisition, development, and maintenance

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 85
You work as a project manager for BlueWell Inc. Your project is running late and you must respond to the risk. Which risk response can you choose that will also cause you to update the human resource management plan?

Real 49
ISC CAP Exam

A. Teamingagreements
B. Crashing the project
C. Transference
D. Fast tracking the project

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 86
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2
B. Level 3
C. Level 5
D. Level 4
E. Level 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 87
You are the project manager for your company and a new change request has been approved for your project. This change request, however, has introduced several new risks to the project. You have communicated these risk events and the project stakeholders understand the possible effects these risks could have on your project. You elect to create a mitigation response for the identified risk events. Where will you record the mitigation response?

A. Risk register
B. Risk log
C. Risk management plan
D. Project management plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 88

ISO 17799 has two parts. The first part is an implementation guide with guidelines on how to build a comprehensive information security infrastructure and the second part is an auditing guide based on requirements that must be met for an organization to be deemed compliant with ISO 17799. What are the ISO 17799 domains?

Each correct answer represents a complete solution. Choose all that apply.

A. Information security policy for the organization
B. Personnel security
C. Business continuity management
D. System architecture management
E. System development and maintenance

Correct Answer: ABCE
Section: (none)
Explanation

Explanation/Reference:
Real 51
ISC CAP Exam

Explanation:

QUESTION 89
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and Accreditation?

Each correct answer represents a complete solution. Choose two.

A. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
C. Certification isthe official management decision given by a senior agency official to authorize operation of an information system.
D. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 90
Amy is the project manager for her company. In her current project the organization has a very low tolerance for risk events that will affect the project schedule. Management has asked Amy to consider the affect of all the risks on the project schedule. What approach can Amy take to create a bias against risks that will affect the schedule of the project?

A. She can have the project team pad their time estimates to alleviate delays in the project schedule.
B. She can shift risk-laden activities that affect the project schedule from the critical path as much as possible.
C. She can create an overall project rating scheme to reflect the bias towards risks that affect the project schedule.
D. She can filter all risks based on their affect on schedule versus other project objectives.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 91
You and your project team are just starting the risk identification activities for a project that is scheduled to last for 18 months. Your project team has already identified a long list of risks that need to be analyzed. How often should you and the project team do risk identification?

A. At least once per month
B. Several times until the project moves into execution
C. It depends on how many risks are initially identified.
D. Identify risks is an iterative process.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 92
Which of the following documents were developed by NIST for conducting Certification & Accreditation (C&A)?

Each correct answer represents a complete solution. Choose all that apply.

A. NIST Special Publication 800-53A
B. NIST Special Publication 800-37A

C. NIST Special Publication 800-59
D. NIST Special Publication 800-53
E. NIST Special Publication 800-37
F. NIST Special Publication 800-60
Real 53
ISC CAP Exam

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: A,C,D,E,F
Explanation:

QUESTION 93
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. Communications Management Plan
B. Risk Management Plan
C. Project Management Plan
D. Risk ResponsePlan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 94
Which of the following individuals informs all C&A participants about life cycle actions, security requirements, and documented user needs?

A. IS program manager
B. Certification Agent
C. User representative
D. DAA

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 95
You are the project manager of the NNH Project. In this project you have created a contingency response that the schedule performance index should be less than 0.93. The NHH Project has a budget at completion of $945,000 and is 45 percent complete though the project should be 49 percent complete. The project has spent $455,897 to reach the 45 percent complete milestone.

What is the project's schedule performance index?

A. 1.06
B. 0.93
C. -$37,800
D. 0.92

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 55
ISC CAP Exam

QUESTION 96
Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

A. Safeguards
B. Preventive controls
C. Detective controls
D. Corrective controls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 97
Which of the following is NOT an objective of the security program?

A. Security plan
B. Security education
C. Security organization
D. Information classification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 98
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some

Real 56
ISC CAP Exam
of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

A. Project communications plan
B. Project management plan
C. Projectcontractual relationship with the vendor
D. Project scope statement

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 99
Penetration testing (also called pen testing) is the practice of testing a computer system, network, or Web application to find vulnerabilities that an attacker could exploit. Which of the following areas can be exploited in a penetration test?

Each correct answer represents a complete solution. Choose all that apply.

A. Race conditions
B. Social engineering
C. Information system architectures
D. Buffer overflows
E. Kernel flaws
F. Trojan horses
G. File and directory permissions

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: A,B,D,E,F,G
Explanation:

QUESTION 100
Which of the following methods of authentication uses finger prints to identify users?

A. PKI
B. Mutual authentication
C. Biometrics
D. Kerberos

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 101
In which of the following Risk Management Framework (RMF) phases is strategic risk assessment planning performed?

A. Phase 0
B. Phase 1
C. Phase 2
D. Phase 3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 102
Which of the following administrative policy controls requires individuals or organizations to be engaged in good business practices relative to the organization's industry?

A. Segregation of duties
Real 58
ISC CAP Exam
B. Separation of duties
C. Need to Know
D. Due care

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 103
Which of the following is a security policy implemented by an organization due to compliance, regulation, or other legal requirements?

A. Advisory policy
B. Informative policy
C. System Security policy
D. Regulatory policy

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 104
Which of the following phases begins with a review of the SSAA in the DITSCAP accreditation?

A. Phase 1
B. Phase 4
C. Phase 3
D. Phase 2

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 105
Which of the following is NOT a type of penetration test?

A. Cursory test
B. Partial-knowledge test
C. Zero-knowledge test
D. Full knowledge test

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 106
Which of the following formulas was developed by FIPS 199 for categorization of an information system?

A. SC information system = {(confidentiality, impact), (integrity, controls), (availability, risk)}
B. SC information system = {(confidentiality, impact), (integrity, impact),(availability, impact)}

C. SC information system = {(confidentiality, controls), (integrity, controls), (availability, controls)}
D. SC information system = {(confidentiality, risk), (integrity, impact), (availability, controls)}

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 60
ISC CAP Exam

QUESTION 107
Which of the following NIST documents defines impact?

A. NIST SP 800-53
B. NIST SP 800-26
C. NIST SP 800-30
D. NIST SP 800-53A

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 108
Which of the following relations correctly describes residual risk?

A. Residual Risk = Threats x Vulnerability x Asset Gap x Control Gap
B. Residual Risk = Threats x Exploit x Asset Value x Control Gap
C. Residual Risk = Threats x Exploit x Asset Value x Control Gap
D. Residual Risk = Threats x Vulnerability x Asset Value x Control Gap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 109
Which of the following is NOT a phase of the security certification and accreditation process?

A. Initiation
B. Security certification
C. Operation
D. Maintenance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 110
In which of the following phases does the SSAA maintenance take place?

A. Phase 3
B. Phase 2
C. Phase 1
D. Phase 4

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 111
In which of the following phases do the system security plan update and the Plan of Action and Milestones (POAM) update take place?

A. Continuous Monitoring Phase
B. Accreditation Phase
C. Preparation Phase
D. DITSCAP Phase

Real 62
ISC CAP Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 112
Which of the following processes is used to protect the data based on its secrecy, sensitivity, or confidentiality?

A. Change Control
B. Data Hiding
C. Configuration Management
D. Data Classification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 113
Which of the following documents is used to provide a standard approach to the assessment of NIST SP 800-53 security controls?

A. NIST SP 800-37
B. NIST SP 800-41
C. NIST SP 800-53A
D. NIST SP 800-66

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 63

QUESTION 114
You are the project manager for your organization. You are working with your key stakeholders in the qualitative risk analysis process. You understand that there is certain bias towards the risk events in the project that you need to address, manage, and ideally reduce. What solution does the PMBOK recommend to reduce the influence of bias during qualitative risk analysis?

A. Establish the definitions of the levels of probability and impact
B. Isolate the stakeholders by project phases to determine their risk bias
C. Involve all stakeholders to vote on the probability and impact of the risk events
D. Provideiterations of risk analysis for true reflection of a risk probability and impact

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 115
Numerous information security standards promote good security practices and define frameworks or systems to structure the analysis and design for managing information security controls. Which of the following are the international information security standards?

Each correct answer represents a complete solution. Choose all that apply.

A. Human resources security
B. Organization of information security
C. Risk assessment and treatment
D. AU audit and accountability

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Real 64
ISC CAP Exam

Explanation:

QUESTION 116

You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

A. Risk management plan
B. Stakeholder management strategy
C. Risk register
D. Lessons learned documentation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 117
Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

A. IFB
B. RFI
C. RFQ
Real 65
ISC CAP Exam
D. RFP

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 118
Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?

A. Computer Fraud and Abuse Act
B. FISMA

C. Lanham Act
D. Computer Misuse Act

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 119
Which of the following is used in the practice of Information Assurance (IA) to define assurance requirements?

A. Classic information security model
B. Communications Management Plan
C. Five Pillars model
D. Parkerian Hexad
Real 66
ISC CAP Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 120
Joan is the project manager of the BTT project for her company. She has worked with her project to create risk responses for both positive and negative risk events within the project. As a result of this process Joan needs to update the project document updates. She has updated the assumptions log as a result of the findings and risk responses, but what other documentation will need to be updated as an output of risk response planning?

A. Lessons learned
B. Scope statement
C. Risk Breakdown Structure
D. Technical documentation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 121
Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Discretionary Access Control
B. Mandatory Access Control
C. Policy Access Control
D. Role-Based Access Control

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 122
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. Risks
C. Costs
D. Quality control concerns

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 123
Which of the following components ensures that risks are examined for all new proposed change requests in the change control system?

A. Risk monitoring and control
B. Scope change control

C. Configuration management
D. Integrated change control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 124
Which of the following classification levels defines the information that, if disclosed to the unauthorized parties, could be reasonably expected to cause exceptionally grave damage to the national security?

A. Secret information
B. Top Secret information
C. Confidential information
D. Unclassified information
Real 68
ISC CAP Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 125
Mary is the project manager of the HGH Project for her company. She and her project team have agreed that if the vendor is late by more than ten days they will cancel the order and hire the NBG Company to fulfill the order. The NBG Company can guarantee orders within three days, but the costs of their products are significantly more expensive than the current vendor. What type of a response strategy is this?

A. Contingent response strategy
B. Expert judgment
C. Internal risk management strategy
D. External risk response

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 126
Which of the following individuals is responsible for monitoring the information system environment for factors that can negatively impact the security of the system and its accreditation?

A. Chief Risk Officer
B. Chief Information Security Officer
C. Information System Owner
D. Chief Information Officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 127
Which of the following is a temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls?

A. IATT
B. ATO
C. IATO
D. DATO

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 128
Fill in the blank with an appropriate word.

________ ensures that the information is not disclosed to unauthorized persons or processes.

A. Confidentiality

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 129
Nancy is the project manager of the NHH project. She and the project team have identified a significant risk in the project during the qualitative risk analysis process. Bob is familiar with the technology that the risk is affecting and proposes to Nancy a solution to the risk event. Nancy tells Bob that she has noted his response, but the risk really needs to pass through the quantitative risk analysis process before creating responses. Bob disagrees and ensures Nancy that his response is most appropriate for the identified risk. Who is correct in this scenario?

A. Bob is correct. Bob is familiar with the technology and the risk event so his response should be Real 70
ISC CAP Exam
implemented.
B. Nancy is correct. Because Nancy is the project manager she can determine the correct procedures for risk analysis and risk responses. In addition, she has noted the risk response that Bob recommends.
C. Nancy is correct. All risks of significant probability and impact should pass the quantitative risk analysis process before risk responses are created.
D. Bob is correct. Not all riskevents have to pass the quantitative risk analysis process to develop effective risk responses.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 130
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. FITSAF
B. TCSEC
C. FIPS
D. SSAA

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 131
The only output of the perform qualitative risk analysis are risk register updates. When the project manager updates the risk register he will need to include several pieces of information including all of the following except for which one?

A. Trends in qualitative risk analysis
B. Risk probability-impact matrix
C. Watchlist of low-priority risks
D. Risks grouped by categories

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 132
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. At every status meeting the project team project risk management is an agenda item.
B. Project risk management happens at every milestone.
C. Project risk management has been concluded with the project planning.
D. Project risk management is scheduled for every monthin the 18-month project.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 133
Rob is the project manager of the IDLK Project for his company. This project has a budget of $5,600,000 and is expected to last 18 months. Rob has learned that a new law may affect how the project is allowed to proceed - even though the organization has already invested over $750,000 in the project. What risk response is the most appropriate for this instance?

A. Transference
B. Mitigation
C. Enhance
D. Acceptance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 72
ISC CAP Exam

Topic 3, Volume C

QUESTION 134
You are the project manager of a large construction project. Part of the project involves the wiring of the electricity in the building your project is creating. You and the project team determine the electrical work is too dangerous to perform yourself so you hire an electrician to perform the work for the project. This is an example of what type of risk response?

A. Transference
B. Mitigation
C. Avoidance
D. Acceptance

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 135
You are the project manager of the GHY project for your organization. You are about to start the qualitative risk analysis process for the project and you need to determine the roles and responsibilities for conducting risk management. Where can you find this information?

A. Risk management plan
Real 73

B. Enterprise environmental factors
C. Staffing management plan
D. Risk register

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 136
The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase?

Each correct answer represents a complete solution. Choose all that apply.

A. Registration
B. Document mission need
C. Negotiation
D. Initial Certification Analysis

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 137
Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process?

A. Senior Agency Information Security Officer
B. Authorizing Official
C. Chief Information Officer
D. Common Control Provider

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 138
In which of the following DIACAP phases is residual risk analyzed?

A. Phase 2
B. Phase 4
C. Phase 5
D. Phase 3
E. Phase 1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 139
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

A. Confidentiality
B. Encryption
C. Integrity
D. Availability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 140
Mark is the project manager of the BFL project for his organization. He and the project team are

Real 75

creating a probability and impact matrix using RAG rating. There is some confusion and disagreement among the project team as to how a certain risk is important and priority for attention should be managed. Where can Mark determine the priority of a risk given its probability and impact?

A. Risk response plan
B. Project sponsor
C. Risk management plan
D. Look-up table

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 141
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls are tested and reviewed?

A. Level 1
B. Level 2
C. Level 4
D. Level 5
E. Level 3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 76
ISC CAP Exam

QUESTION 142
A high-profile, high-priority project within your organization is being created. Management wants you to pay special attention to the project risks and do all that you can to ensure that all of the risks are identified early in the project. Management has to ensure that this project succeeds.

Management's risk aversion in this project is associated with what term?

A. Utility function
B. Risk conscience
C. Quantitativerisk analysis
D. Risk mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 143
Which of the following governance bodies directs and coordinates implementations of the information security program?

A. Information Security Steering Committee
B. Senior Management
C. Business Unit Manager
D. Chief Information Security Officer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 144
What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process?

Each correct answer represents a complete solution. Choose all that apply.

A. Conduct activities related to the disposition of the system data and objects.
B. Execute and update IA implementation plan.
C. Conduct validation activities.
D. Combine validation results in DIACAP scorecard.

Correct Answer: BCD
Section: (none)

Explanation

Explanation/Reference:
Real 77
ISC CAP Exam

Explanation:

QUESTION 145
The phase 0 of Risk Management Framework (RMF) is known as strategic risk assessment planning. Which of the following processes take place in phase 0?

Each correct answer represents a complete solution. Choose all that apply.

A. Review documentation and technical data.
B. Apply classification criteria to rank data assets and related IT resources.
C. Establish criteria that will be used to classify and rank data assets.
D. Identify threats, vulnerabilities, and controls that will be evaluated.
E. Establish criteria that will be used to evaluate threats, vulnerabilities, and controls.

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 146
Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

A. Configuration management
B. Procurement management
C. Risk management
D. Change management
Real 78
ISC CAP Exam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 147
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Safeguard
B. Single Loss Expectancy (SLE)
C. Exposure Factor (EF)
D. Annualized Rate of Occurrence (ARO)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 148
Information Security management is a process of defining the security controls in order to protect information assets. The first action of a management program to implement information security is to have a security program in place. What are the objectives of a security program?

Each correct answer represents a complete solution. Choose all that apply.

A. Security organization
B. System classification
C. Information classification
D. Security education
Real 79
ISC CAP Exam

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 149
Which of the following are the types of access controls?

Each correct answer represents a complete solution. Choose three.

A. Administrative
B. Automatic
C. Technical
D. Physical

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 150
You are the project manager of the NNQ Project for your company and are working you're your project team to define contingency plans for the risks within your project. Mary, one of your project team members, asks what a contingency plan is. Which of the following statements best defines what a contingency response is?

A. Some responses are designed for use only if certain events occur.
B. Some responses have a cost and a time factor to consider for each risk event.
C. Some responses must counteract pending risk events.
D. Quantified risks should always have contingency responses.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 151
Which of the following requires all general support systems and major applications to be fully certified and accredited before these systems and applications are put into production?

Each correct answer represents a part of the solution. Choose all that apply.

A. NIST
B. FIPS

C. Office of Management and Budget (OMB)
D. FISMA

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 152
Which of the following refers to a process that is used for implementing information security?

A. Certification and Accreditation(C&A)
B. Information Assurance (IA)
C. Five Pillars model
D. Classic information security model

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 153
Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

A. Corrective action
B. Technical performance measurement
C. Risk audit
D. Earned value management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 154
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. Project charter
B. Risk management plan
C. Risk register
D. Quality management plan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 155
Joan is a project management consultant and she has been hired by a firm to help them identify risk events within the project. Joan would first like to examine the project documents including the plans, assumptions lists, project files, and contracts. What key thing will help Joan to discover risks within the review of the project documents?

A. The project documents will help the project manager, or Joan, to identify what risk identification approach is best to pursue.
B. Plans that have loose definitions of terms and disconnected approaches will reveal risks.
Real 82
ISC CAP Exam
C. Poorly written requirements will reveal inconsistencies in the project plans and documents.
D. Lack of consistency between the plans and the project requirements and assumptions can be the indicators of risk in the project.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 156
Which of the following are the objectives of the security certification documentation task?

Each correct answer represents a complete solution. Choose all that apply.

A. To prepare the Plan of Action and Milestones (POAM) based on the security assessment
B. To provide the certification findings and recommendations to the information system owner
C. To assemble the final security accreditation package and then submit it to the authorizing o fficial
D. To update the system security plan based on the results of the security assessment

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 157
Which of the following statements about System Access Control List (SACL) is true?

A. It contains a list of any events that are set to audit for that particular object.
B. It is a mechanism for reducing the need for globally unique IP addresses.
Real 83
ISC CAP Exam
C. It contains a list of both users and groups and whatever permissions they have.
D. It exists for each and every permission entry assigned to any object.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 158
You are the project manager for your organization. You are working with your project team to complete the qualitative risk analysis process. The first tool and technique you are using requires that you assess the probability and what other characteristic of each identified risk in the project?

A. Risk owner
B. Risk category
C. Impact
D. Cost

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 159
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?

Real 84
ISC CAP Exam

A. The project's cost management plan can help you to determine what the total cost of the project is allowed to be.
B. The project's cost management plan provides direction on how costs may be changed due to identified risks.
C. The project's cost management plan provides control that may help determine the structure for quantitative analysis of the budget.
D. The project's cost management plan is not an input to the quantitative risk analysis process .

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 160
What NIACAP certification levels are recommended by the certifier?

Each correct answer represents a complete solution. Choose all that apply.

A. Minimum Analysis
B. Basic System Review
C. Detailed Analysis
D. Maximum Analysis
E. Comprehensive Analysis
F. Basic Security Review

Correct Answer: ACEF

Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 161
You work as a project manager for BlueWell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decided, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project which of the following are likely to increase?

A. Quality control concerns
B. Costs
C. Risks
D. Human resource needs

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 85
ISC CAP Exam

QUESTION 162
Which of the following are included in Technical Controls?

Each correct answer represents a complete solution. Choose all that apply.

A. Implementing and maintaining access control mechanisms
B. Password and resource management
C. Configuration of the infrastructure
D. Identification and authentication methods
E. Conducting security-awareness training
F. Security devices

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: A,B,C,D,F
Explanation:

QUESTION 163
You are the project manager of the HJK project for your organization. You and the project team have created risk responses for many of the risk events in the project. A teaming agreement is an example of what risk response?

A. Acceptance
B. Mitigation
C. Sharing
D. Transference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Real 86
ISC CAP Exam

Explanation:

QUESTION 164
Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing?

Each correct answer represents a complete solution. Choose all that apply.

A. Full-box
B. Zero-knowledge test
C. Full-knowledge test
D. Open-box
E. Partial-knowledge test
F. Closed-box

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Answer: B,C,D,E,F
Explanation:

QUESTION 165
The Software Configuration Management (SCM) process defines the need to trace changes, and the ability to verify that the final delivered software has all of the planned enhancements that are supposed to be included in the release. What are the procedures that must be defined for each software project to ensure that a sound SCM process is implemented?

Each correct answer represents a complete solution. Choose all that apply.

Real 87
ISC CAP Exam

A. Configuration status accounting
B. Configuration change control
C. Configuration deployment
D. Configuration audits
E. Configuration identification
F. Configuration implementation

Correct Answer: ABDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

A. FIPS
B. TCSEC
C. SSAA
D. FITSAF

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 167
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment?

Each correct answer represents a part of the solution. Choose all that apply.

A. Information Assurance Manager
B. Designated Approving Authority
C. IS program manager
D. User representative
E. Certification agent

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 168
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

A. Enhance
B. Exploit
C. Acceptance
D. Share

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 169
The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. What are the different types of NIACAP

accreditation?

Each correct answer represents a complete solution. Choose all that apply.

A. System accreditation
B. Type accreditation
C. Site accreditation
D. Secure accreditation

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 89
ISC CAP Exam

QUESTION 170
The risk transference is referred to the transfer of risks to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Which one of the following is NOT an example of the transference risk response?

A. Use of insurance
B. Life cycle costing
C. Warranties
D. Performance bonds

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 171
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 charter
B. Risk register
C. Project scope statement
D. Risk low-level watch list
Real 90
ISC CAP Exam

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 172
BS 7799 is an internationally recognized ISM standard that provides high level, conceptual recommendations on enterprise security. BS 7799 is basically divided into three parts. Which of the following statements are true about BS 7799?

Each correct answer represents a complete solution. Choose all that apply.

A. BS 7799 Part 1 was adopted by ISO as ISO/IEC 27001 in November 2005.
B. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.
C. BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995.
D. BS 7799 Part 3 was published in 2005, covering risk analysis and management.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 173
You work as a project manager for TechSoft Inc. You are working with the project stakeholders onthe qualitative risk analysis process in your project. You have used all the tools to the qualitative risk analysis process in your project. Which of the following techniques is NOT used as a tool in qualitative risk analysis process?

A. Risk Reassessment
B. Risk Categorization
C. Risk Urgency Assessment

D. Risk Data Quality Assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 174
You are the project manager for your organization. You have determined that an activity is too dangerous to complete internally so you hire licensed contractor to complete the work. The contractor, however, may not complete the assigned work on time which could cause delays in subsequent work beginning. This is an example of what type of risk event?

A. Secondary risk
B. Transference
C. Internal
D. Pure risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 175
Tracy is the project manager of the NLT Project for her company. The NLT Project is scheduled to last 14 months and has a budget at completion of $4,555,000. Tracy's organization will receive a bonus of $80,000 per day that the project is completed early up to $800,000. Tracy realizes that

Real 92
ISC CAP Exam
there are several opportunities within the project to save on time by crashing the project work.

Crashing the project is what type of risk response?

A. Mitigation
B. Exploit
C. Enhance
D. Transference

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 176
You work as a project manager for BlueWell Inc. You are about to complete the quantitative risk analysis process for your project. You can use three available tools and techniques to complete this process. Which one of the following is NOT a tool or technique that is appropriate for the quantitative risk analysis process?

A. Quantitative risk analysis andmodeling techniques
B. Data gathering and representation techniques
C. Expert judgment
D. Organizational process assets

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 93
ISC CAP Exam

QUESTION 177
You work as a project manager for TechSoft Inc. You, the project team, and the key project stakeholders have completed a round of quantitative risk analysis. You now need to update the risk register with your findings so that you can communicate the risk results to the project stakeholders - including management. You will need to update all of the following information except for which one?

A. Probability of achieving cost and time objectives
B. Risk distributions within the project schedule
C. Probabilistic analysis of the project
D. Trends in quantitative risk analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 178
Lisa is the project manager of the SQL project for her company. She has completed the risk response planning with her project team and is now ready to update the risk register to reflect the risk response. Which of the following statements best describes the level of detail Lisa should include with the risk responses she has created?

A. The level of detail is set by historical information.
B. The level of detail must define exactly the risk response for each identified risk.
C. The level of detail is set of project risk governance.
D. The level of detail should correspond with the priority ranking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 179
David is the project manager of HGF project for his company. David, the project team, and several key stakeholders have completed risk identification and are ready to move into qualitative risk analysis. Tracy, a project team member, does not understand why they need to complete qualitative risk analysis. Which one of the following is the best explanation for completing qualitative risk analysis?

A. It isa rapid and cost-effective means of establishing priorities for the plan risk responses and lays the foundation for quantitative analysis.
B. It is a cost-effective means of establishing probability and impact for the project risks.
C. Qualitative risk analysis helps segment the project risks, create a risk breakdown structure, and Real 94
ISC CAP Exam
create fast and accurate risk responses.
D. All risks must pass through quantitative risk analysis before qualitative risk analysis.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 180
The Identify Risk process determines the risks that affect the project and document their characteristics. Why should the project team members be

involved in the Identify Risk process?

A. They are the individuals that will have the best responses for identified risks events within the project.
B. They are the individuals that are most affected by the risk events.
C. They are the individuals that will need a sense of ownership and responsibility for the risk e vents.
D. They are the individuals that will most likely cause and respond to the risk events.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 181
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

Real 95
ISC CAP Exam

A. Business continuity plan
B. Continuity of Operations Plan
C. Disaster recovery plan
D. Contingency plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 182
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy
B. User password policy
C. Backup policy
D. Privacy policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 183
You work as a project manager for BlueWell Inc. You are working with your team members on the risk responses in the project. Which risk response will likely cause a project to use the procurement processes?

A. Acceptance
B. Mitigation
C. Exploiting
D. Sharing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 184
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?

A. Level 2
B. Level 5
C. Level 4
D. Level 1
E. Level 3

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 185
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. Harry is correct, because the risk probability and impact considers all objectives of the proj ect.
B. Harry is correct, the risk probability and impact matrix is the only approach to risk assessm ent.
C. Sammy is correct, because sheis the project manager.
D. Sammy is correct, because organizations can create risk scores for each objective of the pr oject.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 97
ISC CAP Exam

QUESTION 186
An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

A. Anonymous
B. Multi-factor
C. Biometrics
D. Mutual

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 187
The Phase 3 of DITSCAP C&A is known as Validation. The goal of Phase 3 is to validate that the preceding work has produced an IS that operates in a specified computing environment. What are the process activities of this phase?

Each correct answer represents a complete solution. Choose all that apply.

A. Perform certification evaluation of the integrated system
B. System development
C. Certification and accreditation decision
D. Develop recommendation to the DAA
E. Continue to review and refine the SSAA

Correct Answer: ACDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 188
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. Risk Management Plan
C. Project ManagementPlan
D. Communications Management Plan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 189
Your organization has named you the project manager of the JKN Project. This project has a BAC of $1,500,000 and it is expected to last 18 months. Management has agreed that if the schedule baseline has a variance of more than five percent then you will need to crash the project. What happens when the project manager crashes a project?

A. Project costs will increase.
B. The amount of hours a resource can be used will diminish.
C. The projectwill take longer to complete, but risks will diminish.
D. Project risks will increase.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 190
Which of the following DoD directives defines DITSCAP as the standard C&A process for the Department of Defense?

A. DoD 8000.1
B. DoD 5200.40
C. DoD 5200.22-M
D. DoD 8910.1

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 191
A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. What are the different types of policies?

Each correct answer represents a complete solution. Choose all that apply.

A. Systematic
B. Informative
C. Regulatory
D. Advisory

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 192
In 2003, NIST developed a new Certification & Accreditation (C&A) guideline known as FIPS 199.

What levels of potential impact are defined by FIPS 199?

Each correct answer represents a complete solution. Choose all that apply.

A. Medium
B. High
C. Low
D. Moderate

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 193
Which types of project tends to have more well-understood risks?

A. State-of-art technologyprojects
B. Recurrent projects
C. Operational work projects
D. First-of-its kind technology projects

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 194
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?

Each correct answer represents a complete solution. Choose all that apply.

A. An ISSO manages the security of the information system that is slated for Certification Real 102
ISC CAP Exam
&Accreditation (C&A).
B. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
C. An ISSE provides advice on the continuous monitoring of the information system.
D. An ISSO takes part in the development activities that are required to implement system ch anges.
E. An ISSE provides advice on the impacts of system changes.

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 195
The Chief Information Officer (CIO), or Information Technology (IT) director, is a job title commonly given to the most senior executive in an enterprise. What are the responsibilities of a Chief Information Officer?

Each correct answer represents a complete solution. Choose all that apply.

A. Proposing the information technology needed by an enterprise to achieve its goals and then working within a budget to implement the plan
B. Preserving high-level communications and working group relationships in an organization
C. Establishing effective continuous monitoring program for the organization
D. Facilitating the sharing of security risk-related information among authorizing officials

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 103
ISC CAP Exam

QUESTION 196
Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

A. It depends on what the outcome of a lawsuit will determine.
B. No, the ZAS Corporation did not complete all of the work.
C. It depends on what the termination clause of the contract stipulates.
D. Yes, the ZAS Corporation did not choose to terminate the contract work.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 197
Mark works as a project manager for TechSoft Inc. Mark, the project team, and the key project stakeholders have completed a round of qualitative risk analysis. He needs to update the risk register with his findings so that he can communicate the risk results to the project stakeholders - including management. Mark will need to update all of the following information except for which one?

A. Watchlist of low-priority risks
B. Prioritized list of quantified risks
C. Risks grouped by categories
D. Trends in qualitative risk analysis

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 198
Which of the following tasks are identified by the Plan of Action and Milestones document?

Each correct answer represents a complete solution. Choose all that apply.

A. The plans that need to be implemented
B. The resources needed to accomplish the elements of the plan
C. Any milestones that are needed in meeting the tasks
D. The tasks that are required to be accomplished
E. Scheduled completion dates for the milestones

Correct Answer: BCDE
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 199
Jenny is the project manager for the NBT projects. She is working with the project team and several subject matter experts to perform the quantitative risk analysis process. During this process she and the project team uncover several risks events that were not previously identified.

What should Jenny do with these risk events?

A. The events should be determined if they need to be accepted or responded to.
B. The events should be entered into qualitative risk analysis.
C. The events should continue on with quantitative risk analysis.
D. The events should be entered into the risk register.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 200
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

Real 105
ISC CAP Exam

A. Authenticity
B. Confidentiality
C. Availability
D. Integrity

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
Explanation:

QUESTION 201
You are the project manager of the BlueStar project in your company. Your company is structured as a functional organization and you report to the functional manager that you are ready to move onto the qualitative risk analysis process. What will you need as inputs for the qualitative risk analysis of the project in this scenario?

A. You will need the risk register, risk management plan, project scope statement, and any relevant organizational process assets.
B. You will need the risk register, risk management plan, outputs of qualitative risk analysis, and any relevant organizational process assets.
C. You will need the risk register, risk management plan, permission from the functional manager, and any relevant organizational process assets.
D. Qualitative risk analysis does not happen through the project manager in a functional struc ture.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Real 106
ISC CAP Exam

Explanation:

QUESTION 202
Henry is the project manager of the QBG Project for his company. This project has a budget of $4,576,900 and is expected to last 18 months to complete. The CIO, a stakeholder in the project, has introduced a scope change request for additional deliverables as part of the project work.

What component of the change control system would review the proposed changes' impact on the features and functions of the project's product?

A. Cost change control system
B. Scope change control system
C. Integrated change control
D. Configuration management system

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 203
Security Test and Evaluation (ST&E) is a component of risk assessment. It is useful in discovering system vulnerabilities. For what purposes is ST&E used?

Each correct answer represents a complete solution. Choose all that apply.

A. To implement the design of system architecture
B. To determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy
C. To assess the degree of consistency between the system documentation and its implement ation
D. To uncover design, implementation, and operational flaws that may allow the violation of security policy

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 204
Elizabeth is a project manager for her organization and she finds risk management to be very difficult for her to manage. She asks you, a lead project manager, at what stage in the project will risk management become easier. What answer best resolves the difficulty of risk management practices and the effort required?

A. Risk management only becomes easier the more often it is practiced.
B. Risk management is an iterative process and never becomes easier.
C. Risk management only becomes easier when the project moves into project execution.
D. Risk management only becomes easier when the project is closed.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 205
Which of the following is NOT an objective of the security program?

A. Security organization

B. Security plan
C. Security education
D. Information classification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Topic 4, Volume D

QUESTION 206
Which of the following RMF phases identifies key threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of the institutional critical assets?

Real 108
ISC CAP Exam

A. Phase 2
B. Phase 1
C. Phase 3
D. Phase 0

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 207
Bill is the project manager of the JKH Project. He and the project team have identified a risk event in the project with a high probability of occurrence and the risk event has a high cost impact on the project. Bill discusses the risk event with Virginia, the primary project customer, and she decides that the requirements surrounding the risk event should be removed from the project. The removal of the requirements does affect the project scope, but it can release the project from the high risk exposure. What risk response has been enacted in this project?

A. Avoidance
B. Acceptance
C. Transference
D. Mitigation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 109
ISC CAP Exam

QUESTION 208
In what portion of a project are risk and opportunities greatest and require intense planning and anticipation of risk events?

A. Planning
B. Executing
C. Closing
D. Initiating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 209
You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.
B. It is a risk that remains after planned risk responses are taken.
C. It is a risk that can not be addressed by a risk response.
D. It is a risk that will remain no matter what type of risk response is offered.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 210
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 planning and quantification of risk responses based on probability and impact of each risk event.
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 review of the risk events with the high probability and the highest impact on the project objectives.
D. Quantitative risk analysis is the process of numerically analyzing the effect of identified risks on overall project objectives.
Real 110
ISC CAP Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 211
Fred is the project manager of the CPS project. He is working with his project team to prioritize the identified risks within the CPS project. He and the team are prioritizing risks for further analysis or action by assessing and combining the risks probability of occurrence and impact.

What process is Fred completing?

A. Risk identification
B. Perform qualitative analysis
C. Perform quantitative analysis
D. Risk Breakdown Structure creation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 212

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. Uncertainty in values such as duration of schedule activities
B. Bias towards risk in new resources
Real 111
ISC CAP Exam
C. Risk probabilityand impact matrixes
D. Risk identification

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 213
Which of the following acts promote a risk-based policy for cost effective security?

Each correct answer represents a part of the solution. Choose all that apply.

A. Clinger-Cohen Act
B. Lanham Act
C. Computer Misuse Act
D. Paperwork Reduction Act (PRA)

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 214
To help review or design security controls, they can be classified by several criteria. One of these criteria is based on time. According to this criteria, which of the following controls are intended to prevent an incident from occurring?

A. Adaptive controls
B. Preventive controls

C. Detective controls
D. Corrective controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 215
You are the project manager for a construction project. The project involves casting of a column in a very narrow space. Because of lack of space, casting it is highly dangerous. High technical skill will be required for casting that column. You decide to hire a local expert team for casting that column. Which of the following types of risk response are you following?

A. Mitigation
Real 112
ISC CAP Exam
B. Avoidance
C. Transference
D. Acceptance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 216
Which of the following statements about the authentication concept of information security management is true?

A. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.
B. It ensures that modifications are not made to data by unauthorized personnel or processes .
C. It establishes the users' identity and ensures that the users are who they say they are.
D. It ensures the reliable and timely access to resources.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 217
NIST SP 800-53A defines three types of interview depending on the level of assessment conducted. Which of the following NIST SP 800-53A interviews consists of informal and ad hoc interviews?

Real 113
ISC CAP Exam

A. Substantial
B. Significant
C. Abbreviated
D. Comprehensive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 218
What are the responsibilities of a system owner?

Each correct answer represents a complete solution. Choose all that apply.

A. Integrates security considerations into application and system purchasing decisions and development projects.
B. Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.
C. Ensures that adequate security is being provided by the necessary controls, password management, remoteaccess controls, operating system configurations, and so on.
D. Ensures that the necessary security controls are in place.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 219
During which of the following processes, probability and impact matrix is prepared?

A. Plan Risk Responses
B. Perform Quantitative Risk Analysis
C. Perform Qualitative Risk Analysis
D. Monitoring and Control Risks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 220
Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. Which of the following statements are true about Certification and

Real 114
ISC CAP Exam
Accreditation?

Each correct answer represents a complete solution. Choose two.

A. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
B. Certification is a comprehensive assessment of the management, operational, and technical security controls inan information system.
C. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 221
Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

A. Hackers

B. Visitors
C. Customers
D. Employees

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 115
ISC CAP Exam

QUESTION 222
You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

A. Risk identification
B. Qualitative risk analysis
C. Risk response implementation
D. Quantitative risk analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 223
Which of the following statements about role-based access control (RBAC) model is true?

A. In this model, the permissions are uniquely assigned to each user account.
B. In this model, a user can access resources according to his role in the organization.
C. In this model, the same permission is assigned to each user account.
D. In this model, the users canaccess resources according to their seniority.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 116
ISC CAP Exam

QUESTION 224
The Project Risk Management knowledge area focuses on which of the following processes?

Each correct answer represents a complete solution. Choose all that apply.

A. Quantitative Risk Analysis
B. Potential Risk Monitoring
C. Risk Monitoring and Control
D. Risk Management Planning

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 225
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

A. Exploit
B. Share
C. Enhance
D. Acceptance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 226
Real 117
ISC CAP Exam
Which of the following persons is responsible for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not?

A. Auditor
B. User
C. Data custodian
D. Data owner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 227
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

A. DITSCAP
B. NIACAP
C. NSA-IAM
D. ASSET

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 228
You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your project. Which risk management process can satisfy management's objective for your project?

A. Qualitative risk analysis
B. Quantitative analysis

C. Historical information
D. Rolling wave planning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 229
Real 118
ISC CAP Exam
Which of the following statements best describes the difference between the role of a data owner and the role of a data custodian?

A. The custodian implements the information classification scheme after the initial assignment by the operations manager.
B. The datacustodian implements the information classification scheme after the initial assignment by the data owner.
C. The data owner implements the information classification scheme after the initial assignment by the custodian.
D. The custodian makes the initialinformation classification assignments, and the operations manager implements the scheme.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 230
Which of the following system security policies is used to address specific issues of concern to the organization?

A. Program policy
B. Issue-specific policy
C. Informative policy
D. System-specific policy

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Real 119
ISC CAP Exam

QUESTION 231
Which of the following individuals is responsible for ensuring the security posture of the organization's information system?

A. Authorizing Official
B. Chief Information Officer
C. Security Control Assessor
D. Common Control Provider

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 232
In which of the following Risk Management Framework (RMF) phases is a risk profile created for threats?

A. Phase 3
B. Phase 1
C. Phase 2
D. Phase 0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 233
Which of the following recovery plans includes a monitoring process and triggers for initiating planned actions?

Real 120
ISC CAP Exam

A. Contingency plan
B. Business continuity plan
C. Disaster recovery plan
D. Continuity of Operations Plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 234
What does RTM stand for?

A. Resource Testing Method
B. Replaced Traceability Matrix
C. Requirements Traceability Matrix
D. Resource Tracking Matrix

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 235
Which of the following NIST documents includes components for penetration testing?

A. NIST SP 800-53
B. NIST SP 800-26
C. NIST SP 800-37
D. NIST SP 800-30
Real 121
ISC CAP Exam

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 236
According to FIPS Publication 199, what are the three levels of potential impact on organizations in the event of a compromise on confidentiality, integrity, and availability?

A. Confidential, Secret, and High
B. Minimum, Moderate, and High
C. Low, Normal, and High
D. Low, Moderate, and High

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 237
Which of the following is a risk that is created by the response to another risk?

A. Secondary risk
B. Residual risk
C. Positive risk
D. Negative risk

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 122
ISC CAP Exam

QUESTION 238
Which of the following processes has the goal to ensure that any change does not lead to reduced or compromised security?

A. Risk management
B. Security management
C. Configuration management
D. Changecontrol management

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 239
In which of the following phases does the SSAA maintenance take place?

A. Phase 4
B. Phase 2
C. Phase 1
D. Phase 3

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 240
In which of the following phases do the system security plan update and the Plan of Action and Milestones (POAM) update take place?

A. Continuous Monitoring Phase
B. Accreditation Phase
C. Preparation Phase
D. DITSCAP Phase

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

QUESTION 241
In which of the following phases does the change management process start?

A. Phase 2
B. Phase 1
C. Phase 4
D. Phase 3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 242
Which of the following individuals is responsible for configuration management and control task?

A. Authorizing official
B. Information system owner
C. Chief information officer
D. Common control provider

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 243
In which of the following DITSCAP phases is the SSAA developed?

A. Phase 2
B. Phase 4
C. Phase 1
D. Phase 3

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 125
ISC CAP Exam

QUESTION 244
Which of the following is used throughout the entire C&A process?

A. DAA
B. DITSCAP
C. SSAA
D. DIACAP

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 245
What does OCTAVE stand for?

A. Operationally Computer Threat, Asset, and Vulnerability Evaluation
B. Operationally Critical Threat, Asset, and Vulnerability Evaluation
C. Operationally Computer Threat, Asset, and Vulnerability Elimination
D. Operationally Critical Threat, Asset, and Vulnerability Elimination

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 246

Which of the following C&A professionals plays the role of an advisor?

A. Information System Security Engineer (ISSE)
B. Chief Information Officer (CIO)
C. Authorizing Official
D. Information Owner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 247
In which of the following elements of security does the object retain its veracity and is intentionally

Real 126
ISC CAP Exam
modified by the authorized subjects?

A. Integrity
B. Nonrepudiation
C. Availability
D. Confidentiality

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 248
Which of the following recovery plans includes a monitoring process and triggers for initiating planned actions?

A. Business continuity plan
B. Contingency plan
C. Continuity of Operations Plan
D. Disaster recovery plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 249
Which of the following NIST publications defines impact?

A. NIST SP 800-41
B. NIST SP 800-37
C. NIST SP 800-30
D. NIST SP 800-53

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 250
Which of the following NIST documents defines impact?

A. NIST SP 800-26
B. NIST SP 800-53A
Real 127
ISC CAP Exam
C. NIST SP 800-53
D. NIST SP 800-30

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 251

Which of the following relations correctly describes total risk?

A. Total Risk = Threats x Vulnerability x Asset Value
B. Total Risk = Viruses x Vulnerability x Asset Value
C. Total Risk = Threats x Exploit x Asset Value
D. Total Risk = Viruses x Exploit x Asset Value

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 252
Which of the following individuals is responsible for the final accreditation decision?

A. Certification Agent
B. User Representative
C. Information System Owner
D. Risk Executive

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Real 128
ISC CAP Exam

Explanation:

QUESTION 253
Which of the following individuals makes the final accreditation decision?

A. DAA
B. ISSO
C. CIO
D. CISO

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 254
A ________ points to a statement in a policy or procedure that helps determine a course of action.

A. Comment
B. Guideline
C. Procedure
D. Baseline

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 255
For which of the following reporting requirements are continuous monitoring documentation reports used?

A. FISMA
B. NIST
C. HIPAA
D. FBI

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 256
Which of the following individuals is responsible for configuration management and control task?

A. Commoncontrol provider

B. Information system owner
C. Authorizing official
D. Chief information officer

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 257
Which of the following documents is used to provide a standard approach to the assessment of NIST SP 800-53 security controls?

A. NIST SP 800-53A
B. NIST SP 800-66
C. NIST SP 800-41
D. NIST SP 800-37

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 258
Which of the following guidance documents is useful in determining the impact level of a particular threat on agency systems?

A. NIST SP 800-41
Real 130
ISC CAP Exam
B. NIST SP 800-37
C. FIPS 199
D. NIST SP 800-14

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 259
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

A. DoD 5200.22-M
B. DoD 5200.1-R
C. DoD 8910.1
D. DoDD 8000.1
E. DoD 7950.1-M

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 260
Management wants you to create a visual diagram of what resources will be utilized in the project deliverables. What type of a chart is management asking you to create?

Real 131
ISC CAP Exam

A. Work breakdown structure
B. Roles and responsibility matrix
C. Resource breakdown structure
D. RACI chart

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 261
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a

terminal/Web site. Which of the following is violated in a shoulder surfing attack?

A. Authenticity
B. Integrity
C. Availability
D. Confidentiality

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 262
In which type of access control do user ID and password system come under?

Real 132
ISC CAP Exam

A. Administrative
B. Technical
C. Physical
D. Power

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 263
There are seven risk responses for any project. Which one of the following is a valid risk response for a negative risk event?

A. Enhance
B. Exploit
C. Acceptance
D. Share

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 264
Which of the following DITSCAP phases validates that the preceding work has produced an IS that operates in a specified computing environment?

A. Phase 3
Real 133
ISC CAP Exam
B. Phase 2
C. Phase 4
D. Phase 1

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 265
The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE?

Each correct answer represents a complete solution. Choose all that apply.

A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
B. An ISSO takes part in the development activities that are required to implement system ch anges.
C. An ISSE provides advice on the continuous monitoring of the information system.
D. An ISSE provides advice on the impacts of system changes.
E. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Real 134
ISC CAP Exam

QUESTION 266
Which one of the following is the only output for the qualitative risk analysis process?

A. Enterprise environmental factors
B. Project management plan
C. Risk register updates
D. Organizational process assets

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 267
You work as a project manager for BlueWell Inc. There has been a delay in your project work that is adversely affecting the project schedule. You decided, with your stakeholders' approval, to fast track the project work to get the project done faster. When you fast track the project which of the following are likely to increase?

A. Risks
B. Human resource needs
C. Quality control concerns
D. Costs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 135
ISC CAP Exam

QUESTION 268

An authentication method uses smart cards as well as usernames and passwords for authentication. Which of the following authentication methods is being referred to?

A. Anonymous
B. Multi-factor
C. Biometrics
D. Mutual

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 269
Which of the following is NOT an objective of the security program?

A. Security organization
B. Security plan
C. Security education
D. Information classification

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 270
Real 136
ISC CAP Exam
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

A. Project contractual relationship with the vendor
B. Project communications plan

C. Project management plan
D. Project scope statement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 271
During which of the following processes, probability and impact matrix is prepared?

A. Plan Risk Responses
B. Perform Quantitative Risk Analysis
C. Perform Qualitative Risk Analysis
D. Monitoring and Control Risks

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 272
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. Symptoms
B. Cost of the project
C. Warning signs
D. Risk rating

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 273
Which of the following is used to indicate that the software has met a defined quality level and is ready for mass distribution either by electronic means or by physical media?

A. DAA
B. RTM
C. ATM
D. CRO

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 274
Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

A. Configuration management
B. Procurement management
C. Change management
D. Risk management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 275
Which of the following is a standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system?

A. TCSEC
B. FIPS

C. SSAA
D. FITSAF

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

QUESTION 276
Which of the following statements correctly describes DIACAP residual risk?

A. It is the remaining risk to the information system after risk palliation has occurred.
B. It is a process of security authorization.
C. It is the technical implementation of the security design.
D. It is used to validate the information system.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Real 139