Number: CAP
Passing Score: 800
Time Limit: 120
File Version: 6.0

Exam Code: CAP
Exam Name: Certified Authorization Professional

Exam A

QUESTION 1
Which of the following processes has the goal to ensure that any change does not lead to reduced or compromised security?

A. Change control management
B. Security management
C. Configuration management
D. Risk management

Correct Answer: A
Section:

QUESTION 2
Which of the following is not a part of Identify Risks process?

A. System or process flow chart
B. Influence diagram
C. Decision tree diagram
D. Cause and effect diagram

Correct Answer: C
Section:

QUESTION 3
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:

QUESTION 4
Harry is a project manager of a software development project. In the early stages of planning, he and the stakeholders operated with the belief that the software they were developing would work with their organization's current computer operating system. Now that the project team has started developing the software it has become apparent that the software will not work with nearly half of the organization's computer operating systems. The incorrect belief Harry had in the software compatibility is an example of what in project management?

A. Issue
B. Risk
C. Constraint
D. Assumption

Correct Answer: D
Section:

QUESTION 5
Which of the following statements about Discretionary Access Control List (DACL) is true?

A. It is a rule list containing access control entries.
B. It specifies whether an audit activity should be performed when an object attempts to access a resource.
C. It is a unique number that identifies a user, group, and computer account.
D. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.

Correct Answer: D
Section:

QUESTION 6
Which types of project tends to have more well-understood risks?

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

Correct Answer: B
Section:

QUESTION 7
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 & 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: A, C, E
Section:

QUESTION 8
Which of the following processes is described in the statement below?
"This is the process of numerically analyzing the effect of identified risks on overall project objectives."

A. Identify Risks
B. Perform Quantitative Risk Analysis
C. Perform Qualitative Risk Analysis
D. Monitor and Control Risks

Correct Answer: B
Section:

QUESTION 9
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:

QUESTION 10
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:

QUESTION 11
Which of the following assessment methods is used to review, inspect, and analyze assessment objects?

A. Testing
B. Examination
C. Interview
D. Debugging

Correct Answer: B
Section:

QUESTION 12
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:

QUESTION 13
What is the objective of the Security Accreditation Decision task?

A. To determine whether the agency-level risk is acceptable or not.
B. To make an accreditation decision
C. To accredit the information system
D. To approve revisions of NIACAP

Correct Answer: A
Section:

QUESTION 14
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. Provide iterations of risk analysis for true reflection of a risk probability and impact

Correct Answer: A
Section:

QUESTION 15
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: A, B, C
Section:

QUESTION 16
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:

QUESTION 17
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:

QUESTION 18
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.

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

Correct Answer: C, D, E, F
Section:

QUESTION 19
Mark works as a Network Administrator for NetTech Inc. He wants users to access only those resources that are required for them. Which of the following access control models will he use?

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

Correct Answer: B
Section:

QUESTION 20
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. FITSAF
B. FIPS
C. TCSEC
D. SSAA

Correct Answer: D
Section:

QUESTION 21
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.
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:

QUESTION 22
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:

QUESTION 23
Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?

A. Definition, Validation, Verification, and Post Accreditation
B. Verification, Definition, Validation, and Post Accreditation
C. Verification, Validation, Definition, and Post Accreditation
D. Definition, Verification, Validation, and Post Accreditation

Correct Answer: D
Section:

QUESTION 24
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.

A. Post-Authorization
B. Pre-certification
C. Post-certification
D. Certification

E. Authorization

Correct Answer: A, B, D, E
Section:

QUESTION 25
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: A, D
Section:

QUESTION 26
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. FISMA
D. Office of Management and Budget (OMB)

Correct Answer: C, D
Section:

QUESTION 27
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: B, C, D
Section:

QUESTION 28
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: A, B, C
Section:

QUESTION 29
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.

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

Correct Answer: A, B, C, D
Section:

QUESTION 30
Which of the following is a subset discipline of Corporate Governance focused on information security systems and their performance and risk management?

A. Lanham Act
B. ISG
C. Clinger-Cohen Act
D. Computer Misuse Act

Correct Answer: B
Section:

QUESTION 31
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 risk is always in the future.

Correct Answer: D
Section:

QUESTION 32
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:

QUESTION 33
Where can a project manager find risk-rating rules?

A. Risk probability and impact matrix
B. Organizational process assets
C. Enterprise environmental factors
D. Risk management plan

Correct Answer: B
Section:

QUESTION 34
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

Correct Answer: D
Section:

QUESTION 35
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:

QUESTION 36
Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?

A. Authorizing Official
B. Chief Risk Officer (CRO)
C. Chief Information Officer (CIO)
D. Information system owner

Correct Answer: D
Section:

QUESTION 37
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
C. Requested changes
D. Risk audits

Correct Answer: C
Section:

QUESTION 38
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?

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

Correct Answer: B
Section:

QUESTION 39
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: B, C, D
Section:

QUESTION 40
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. 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:

QUESTION 41
What are the subordinate tasks of the Initiate and Plan IA C&A phase of the DIACAP process?
Each correct answer represents a complete solution. Choose all that apply.

A. Develop DIACAP strategy.
B. Assign IA controls.
C. Assemble DIACAP team.
D. Initiate IA implementation plan.
E. Register system with DoD Component IA Program.
F. Conduct validation activity.

Correct Answer: A, B, C, D, E
Section:

QUESTION 42
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: B, C, D, E, F
Section:

QUESTION 43
Neil works as a project manager for SoftTech Inc. He is working with Tom, the COO of his company, on several risks within the project. Tom understands that through qualitative analysis Neil has identified many risks in the project. Tom's concern, however, is that the priority list of these risk events are sorted in "high-risk," "moderate-risk," and "low-risk" as conditions apply within the project. Tom wants to know that is there any other objective on which Neil can make the priority list for project risks. What will be Neil's reply to Tom?

A. Risk may be listed by the responses in the near-term
B. Risks may be listed by categories

C. Risks may be listed by the additional analysis and response
D. Risks may be listed by priority separately for schedule, cost, and performance

Correct Answer: D
Section:

QUESTION 44
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:

QUESTION 45
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.

Correct Answer: B
Section:

QUESTION 46
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
C. Risk trigger
D. Risk event

Correct Answer: C
Section:

QUESTION 47
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:

QUESTION 48
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.
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. User
C. Owner
D. Custodian

Correct Answer: D
Section:

QUESTION 49
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:

QUESTION 50
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:

QUESTION 51
Which of the following refers to the ability to ensure that the data is not modified or tampered with?

A. Confidentiality
B. Availability
C. Integrity
D. Non-repudiation

Correct Answer: C
Section:

QUESTION 52
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:

QUESTION 53
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:

QUESTION 54
System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.

A. Pre-certification
B. Certification
C. Post-certification
D. Authorization
E. Post-Authorization

Correct Answer: A, B, D, E
Section:

QUESTION 55
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:

QUESTION 56
Risks with low ratings of probability and impact are included on a ____ for future monitoring.

A. Watchlist
B. Risk alarm
C. Observation list
D. Risk register

Correct Answer: A
Section:

QUESTION 57
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: A, B, C, D, E, G
Section:

QUESTION 58
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:

QUESTION 59

In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test
B. Walk-through test
C. Penetration test
D. Paper test

Correct Answer: C
Section:

QUESTION 60
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:

QUESTION 61
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:

QUESTION 62
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

Correct Answer: C
Section:

QUESTION 63
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:

QUESTION 64
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:

QUESTION 65
Thomas is a key stakeholder in your project. Thomas has requested several changes to the project scope for the project you are managing. Upon review of the proposed changes, you have discovered that these new requirements are laden with risks and you recommend to the change control board that the changes be excluded from the project scope. The change control board agrees with you. What component of the change control system communicates the approval or denial of a proposed change request?

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

Correct Answer: D
Section:

QUESTION 66
Which of the following assessment methodologies defines a six-step technical security evaluation?

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

Correct Answer: D
Section:

QUESTION 67
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:

QUESTION 68
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?

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

Correct Answer: B
Section:

QUESTION 69
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-Cohen Act
D. Paperwork Reduction Act

Correct Answer: C
Section:

QUESTION 70
Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review?

A. The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.
B. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.
C. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.
D. The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.

Correct Answer: D
Section:

QUESTION 71
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. RTM

B. CRO
C. DAA
D. ATM

Correct Answer: A
Section:

QUESTION 72
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 create an overall project rating scheme to reflect the bias towards risks that affect the project schedule.
C. She can filter all risks based on their affect on schedule versus other project objectives.
D. She can shift risk-laden activities that affect the project schedule from the critical path as much as possible.

Correct Answer: B
Section:

QUESTION 73
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:

QUESTION 74
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. Project management plan
B. Risk management plan
C. Risk log
D. Risk register

Correct Answer: D
Section:

QUESTION 75
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:

QUESTION 76
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:

QUESTION 77
Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?

A. Stakeholder register
B. Risk register
C. Project scope statement
D. Risk management plan

Correct Answer: A
Section:

QUESTION 78
Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

A. The Supplier Manager
B. The IT Service Continuity Manager
C. The Service Catalogue Manager
D. The Configuration Manager

Correct Answer: A
Section:

QUESTION 79
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:

QUESTION 80
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 facility and different departments

Correct Answer: A, B, E, F
Section:

QUESTION 81
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:

QUESTION 82
Which one of the following is the only output for the qualitative risk analysis process?

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

Correct Answer: B
Section:

QUESTION 83
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 the current project.
D. You will use organizational process assets for information from prior similar projects.

Correct Answer: C
Section:

QUESTION 84
Beth is the project manager of the BFG Project for her company. In this project Beth has decided to create a contingency response based on the performance of the project schedule. If the project schedule variance is greater than $10,000 the contingency plan will be implemented. What is the formula for the schedule variance?

A. SV=EV-PV
B. SV=EV/AC
C. SV=PV-EV
D. SV=EV/PV

Correct Answer: A
Section:

QUESTION 85
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: C, D
Section:

QUESTION 86
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:

QUESTION 87
What project management plan is most likely to direct the quantitative risk analysis process for a project in a matrix environment?

A. Staffing management plan
B. Risk analysis plan
C. Human resource management plan
D. Risk management plan

Correct Answer: D
Section:

QUESTION 88
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:

QUESTION 89
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:

QUESTION 90
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.
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:

QUESTION 91
Which of the following statements about the availability concept of Information security management is true?

A. It ensures that modifications are not made to data by unauthorized personnel or processes .
B. It ensures reliable and timely access to resources.
C. It determines actions and behaviors of a single individual within a system.
D. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Correct Answer: B
Section:

QUESTION 92
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: A, B, C, D
Section:

QUESTION 93
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.
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:

QUESTION 94
Kelly is the project manager of the BHH project for her organization. She is completing the risk identification process for this portion of her project. Which one of the following is the only thing that the risk identification process will create for Kelly?

A. Project document updates
B. Risk register updates
C. Change requests
D. Risk register

Correct Answer: D
Section:

QUESTION 95
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:

QUESTION 96
You are preparing to complete the quantitative risk analysis process with your project team and several subject matter experts. You gather the necessary inputs including the project's cost management plan. Why is it necessary to include the project's cost management plan in the preparation for the quantitative risk analysis process?

A. The project's cost management plan 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:

QUESTION 97
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: A, C, E, F
Section:

QUESTION 98
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:

QUESTION 99

Information Security management is a process of defining the security controls in order to protect information assets. What are the security management responsibilities?
Each correct answer represents a complete solution. Choose all that apply.

A. Evaluating business objectives, security risks, user productivity, and functionality requirem ents
B. Determining actual goals that are expected to be accomplished from a security program
C. Defining steps to ensure that all the responsibilities are accounted for and properly address ed
D. Determining objectives, scope, policies, priorities, standards, and strategies

Correct Answer: A, B, C, D
Section:

QUESTION 100
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: A, B, C, D, F
Section:

QUESTION 101
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:

QUESTION 102
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: B, C, D, E, F
Section:

QUESTION 103
You are the project manager for TTP project. You are in the Identify Risks process. You have to create the risk register. Which of the following are included in the risk register?
Each correct answer represents a complete solution. Choose two.

A. List of potential responses
B. List of identified risks
C. List of mitigation techniques
D. List of key stakeholders

Correct Answer: A, B
Section:

QUESTION 104
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.

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

Correct Answer: A, B, D, E
Section:

QUESTION 105
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:

QUESTION 106
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: B, C, D, E
Section:

QUESTION 107
Which of the following processes is described in the statement below?
"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Perform Quantitative Risk Analysis
B. Perform Qualitative Risk Analysis
C. Monitor and Control Risks
D. Identify Risks

Correct Answer: C
Section:

QUESTION 108
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:

QUESTION 109
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: A, B, C
Section:

QUESTION 110
You are the project manager of the GHY Project for your company. You have completed the risk response planning with your project team. You now need to update the WBS. Why would the project manager need to update the WBS after the risk response planning process? Choose the best answer.

A. Because of risks associated with work packages
B. Because of work that was omitted during the WBS creation
C. Because of risk responses that are now activities
D. Because of new work generated by the risk responses

Correct Answer: D
Section:

QUESTION 111
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:

QUESTION 112
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

Correct Answer: B
Section:

QUESTION 113
Which of the following is a risk response planning technique associated with threats that seeks to reduce the probability of occurrence or impact of a risk to below an acceptable threshold?

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

Correct Answer: C
Section:

QUESTION 114
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: B, C, D
Section:

QUESTION 115
Gary is the project manager for his organization. He is working with the project stakeholders on the project requirements and how risks may affect their project. One of the stakeholders is confused about what constitutes risks in the project. Which of the following is the most accurate definition of a project risk?

A. It is an uncertain event that can affect the project costs.
B. It is an uncertain event or condition within the project execution.
C. It is an uncertain event that can affect at least one project objective.
D. It is an unknown event that can affect the project scope.

Correct Answer: C
Section:

QUESTION 116
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:

QUESTION 117
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:

QUESTION 118

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 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:

QUESTION 119
Diana is the project manager of the QPS project for her company. In this project Diana and the project team have identified a pure risk. Diana and the project team decided, along with the key stakeholders, to remove the pure risk from the project by changing the project plan altogether. What is a pure risk?

A. It is a risk event that only has a negative side, such as loss of life or limb.
B. It is a risk event that cannot be avoided because of the order of the work.
C. It is a risk event that is created by a risk response.
D. It is a risk event that is generated due to errors or omission in the project work.

Correct Answer: A
Section:

QUESTION 120
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 and modeling techniques
B. Data gathering and representation techniques
C. Expert judgment
D. Organizational process assets

Correct Answer: D
Section:

QUESTION 121
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:

QUESTION 122
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:

QUESTION 123
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 is a 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 create fast and accurate risk responses.
D.

Correct Answer: A
Section:
Explanation:
A. It is a 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 create fast and accurate risk responses.
D. All risks must pass through quantitative risk analysis before qualitative risk analysis.
Answer: A
Explanation:

QUESTION 124
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:

QUESTION 125
Which of the following NIST Special Publication documents provides a guideline on questionnaires and checklists through which systems can be evaluated for compliance against specific control objectives?

A. NIST SP 800-53A

B. NIST SP 800-26
C. NIST SP 800-53
D. NIST SP 800-59
E. NIST SP 800-60
F. NIST SP 800-37

Correct Answer: B
Section:

QUESTION 126
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?

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

Correct Answer: D
Section:

QUESTION 127
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:

QUESTION 128
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:

QUESTION 129
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. System architecture management
C. Business continuity management
D. System development and maintenance
E. Personnel security

Correct Answer: A, C, D, E
Section:

QUESTION 130
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:

QUESTION 131
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 she is the project manager.
D. Sammy is correct, because organizations can create risk scores for each objective of the pr oject.

Correct Answer: D
Section:

QUESTION 132
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:

QUESTION 133
Which of the following risk responses delineates that the project plan will not be changed to deal with the risk?

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

Correct Answer: A
Section:

QUESTION 134
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

A. Protect society, the commonwealth, and the infrastructure.
B. Act honorably, honestly, justly, responsibly, and legally.
C. Provide diligent and competent service to principals.
D. Give guidance for resolving good versus good and bad versus bad dilemmas.

Correct Answer: A, B, C
Section:

QUESTION 135
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: A, C, D, E
Section:

QUESTION 136
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 Management Plan
D. Communications Management Plan

Correct Answer: D
Section:

QUESTION 137

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 project will take longer to complete, but risks will diminish.
D. Project risks will increase.

Correct Answer: A
Section:

QUESTION 138
Which of the following individuals makes the final accreditation decision?

A. ISSE
B. DAA
C. CRO
D. ISSO

Correct Answer: B
Section:

QUESTION 139
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:

QUESTION 140
Virginia is the project manager for her organization. She has hired a subject matter expert to interview the project stakeholders on certain identified risks within the project. The subject matter expert will assess the risk event with what specific goal in mind?

A. To determine the bias of the risk event based on each person interviewed
B. To determine the probability and cost of the risk event
C. To determine the validity of each risk event
D. To determine the level of probability and impact for each risk event

Correct Answer: D
Section:

QUESTION 141
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: B, C, D
Section:

QUESTION 142
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: A, B, C
Section: