Question #1 *Topic 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

Suggested Answer: *C*

Community vote distribution

A (100%)

xBowseRx 2 years, 5 months ago

Selected Answer: A

Only the Senior Agency Information Security Officer should be regularly participating in the configuration management process.

upvoted 1 times

Question #2 *Topic 1*

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

Suggested Answer: *ACD*

Darnetonly 5 years, 2 months ago

In your response to the responsibilities of a CIO you stated "Preserves high- level communications and working group relationships in an organization" which is option A, so why did you it's incorrect? Please eleborate

upvoted 1 times

xBowseRx 2 years, 5 months ago

I believe he mis-spoke. He said A is incorrect, followed by re-stating what option B was. So A, C, and D are all correct.

upvoted 1 times

Ramnik 5 years, 4 months ago

Explanation of this answer:
A Chief Information Officer (CIO) plays the role of a leader. The responsibilities of a Chief Information Officer are as follows: Establishes effective continuous monitoring program for the organization. Facilitates continuous monitoring process for the organizations. Preserves high- level communications and working group relationships in an organization. Confirms that information systems are covered by a permitted security plan and monitored throughout the System Development Life Cycle (SDLC). Manages and delegates decisions to employees in large enterprises. Proposes the information technology needed by an enterprise to achieve its goals and then works within a budget to implement the plan. Answer: A is incorrect. A Risk Executive facilitates the sharing of security risk-related information among authorizing officials.

upvoted 3 times

Question #3 *Topic 1*

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 provides advice on the impacts of system changes.

B. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).

C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).

D. An ISSO takes part in the development activities that are required to implement system changes.

E. An ISSE provides advice on the continuous monitoring of the information system.

Suggested Answer: *ACE*

Ramnik 5 years, 4 months ago

Explanation:

An Information System Security Officer (ISSO) plays the role of a supporter. The responsibilities of an Information System Security Officer (ISSO) are as follows: Manages the security of the information system that is slated for Certification & Accreditation (C&A). Insures the information systems configuration with the agency's information security policy. Supports the information system owner/information owner for the completion of security-related responsibilities. Takes part in the formal configuration management process. Prepares Certification & Accreditation (C&A) packages. An Information System Security Engineer (ISSE) plays the role of an advisor. The responsibilities of an Information System Security Engineer are as follows:
Provides view on the continuous monitoring of the information system. Provides advice on the impacts of system changes. Takes part in the configuration management process. Takes part in the development activities that are required to implement system changes. Follows approved system changes.

upvoted 2 times

Question #4 *Topic 1*

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)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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

A. FITSAF

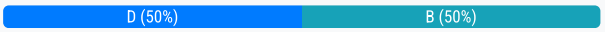
B. FIPS 102

C. OCTAVE

D. DITSCAP

Suggested Answer: *B*

Community vote distribution



Janusguru 9 months, 3 weeks ago

Selected Answer: B

FIPS 102 outlines a six-step process for computer security certification and accreditation. These steps include planning, data collection, basic evaluation, detailed evaluation, reporting findings, and accreditation.

, DITSCAP follows a four-phase process—Definition, Verification, Validation, and Post-Accreditation. While it involves technical security evaluations, it does not align with a six-step structure.

upvoted 1 times

Capkiz 11 months, 2 weeks ago

Selected Answer: D

DITSCAP (Data Interface Technical Security Certification and Accreditation Program) is a six-step technical security evaluation methodology used to assess the security of information systems and networks.

While others may be risk assessment methodologies, they do not define a six-step technical security evaluation methodology.

upvoted 1 times

Question #6 *Topic 1*

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

Suggested Answer: *CDEF*

Ramnik 1 year, 3 months ago

Definition, Verification, Validation, and Post Accreditation - I don't think re-accreditation makes any sense here.

upvoted 4 times

Ramnik 1 year, 3 months ago

https://flylib.com/books/en/1.564.1/understanding_certification_and_accreditation.html#fastmenu_8

Phase 4, post-accreditation, contains activities required to continue to operate and manage the system so that it will maintain an acceptable level of residual risk. Post-accreditation activities must include ongoing maintenance of the SSAA, system operations, security operations, change management, and compliance validation. The other answers relate to Phase 1.

upvoted 1 times

Gabby65 1 year, 4 months ago

Why inst accreditation included if reaccreditation is included?

upvoted 1 times

Question #7 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

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

Suggested Answer: *ABDE*

Ramnik 1 year, 4 months ago

The creation of System Authorization Plan (SAP) is mandated by System Authorization. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. It consists of four phases: Phase 1 - Pre-certification Phase 2 - Certification Phase 3 - Authorization Phase 4 - Post-Authorization

upvoted 3 times

Question #13 *Topic 1*

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.

Suggested Answer: *AD*

Ramnik 1 year, 4 months ago

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. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

upvoted 1 times

Question #14 *Topic 1*

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)

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

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

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

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

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

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

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

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.

Suggested Answer: *D*

Community vote distribution

C (100%)

fortune 1 year, 4 months ago

If it occurs. The uncertain event or condition may or may not occur. If a threat occurs, it becomes an issue or problem. If an opportunity occurs, it becomes a benefit. So, risks are things that may occur; issues and benefits are things that have occurred.

upvoted 2 times

SusanGlenn5 1 year, 6 months ago

Selected Answer: C

It's c

upvoted 1 times

kyle942 2 years ago

A project risk is an uncertain event that may or may not occur during a project. Contrary to our everyday idea of what "risk" means, a project risk could have either a negative or a positive effect on progress towards project objectives.

upvoted 2 times

Ramnik 3 years, 10 months ago

As per PMP-PMI, the answer should be C agree with yellos "Project risk happens throughout the project. How can someone determine it will happen in future.

upvoted 1 times

yellos 3 years, 11 months ago

How can Project Risk happen in the future? I do not understand this? Project risk happens throughout the project.

upvoted 3 times

Question #20 *Topic 1*

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

Suggested Answer: *C*

Ramnik 1 year, 3 months ago

Risk utility function is assigned to the low-level of stakeholder tolerance in this project. The risk utility function describes a person's or organization's willingness to accept risk. It is synonymous with stakeholder tolerance to risk.
Risk utility function facilitates the selection and acceptance of risk and provides opportunity to merge the approach with setting thresholds of risk acceptability and using utility-risk ratios if necessary. Answer: B is incorrect. Risk avoidance is a risk response to avoid negative risk events. Answer: A is incorrect. This is not a valid project management and risk management term. Answer: D is incorrect. Risk-reward describes the balance between accepting risks and the expected reward for the risk event. Risk-reward mentality is not a valid project management term.

upvoted 3 times

Question #21 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

rabbasi41 1 year ago

Selected Answer: D

The inputs to the Perform Quantitative Risk Analysis process are defined in the PMBOK Guide and include:

Risk register: Contains identified risks and related information.
Cost management plan: Provides information on the project's budget and cost-related constraints, useful for financial analysis of risks.
Risk management plan: Outlines how risk management activities will be conducted.
Schedule management plan: Provides details about the project's schedule for analyzing time-related risks.
Enterprise environmental factors (EEFs) are not a specific input to this process. While EEFs influence many project management processes, they are not listed as a direct input for performing quantitative risk analysis.

upvoted 1 times

kyle942 1 year, 6 months ago

Organizational process assets

Project Management plan
Cost management plan
Schedule management plan
Risk register
Enterprise Environmental Factors

upvoted 1 times

Question #23 *Topic 1*

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

Suggested Answer: *D*

Community vote distribution

D (100%)

rabbasi41 1 year ago

Selected Answer: D

Creating a chart that identifies risk probability, impact, and the financial amount associated with each risk event typically results in the determination of a contingency reserve. This reserve is a financial buffer set aside to address the potential costs of identified risks that may occur. It is derived from a quantitative risk analysis that assigns monetary values to the risks.

upvoted 1 times

CapTest 1 year, 6 months ago

D is the correct answer:

Contingency reserve is used when a risk occurs as part of the risk response strategy. The actual impact of the risk is added to the cost or schedule.

upvoted 2 times

CyberRomeo 1 year, 10 months ago

The right answer here is B

upvoted 1 times

Question #24 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

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

Suggested Answer: *B*

Ramnik 1 year, 4 months ago

The various DoD directives are as follows:
DoD 5200.1-R: This DoD directive refers to the 'Information Security Program Regulation'. DoD 5200.22-M: This DoD directive refers the 'National Industrial Security Program Operating Manual'. DoD 7950.1-M: This DoD directive refers to the 'Defense Automation Resources Management Manual'. DoDD 8000.1: This DoD directive refers to the 'Defense Information Management (IM) Program'. DoD 8910.1: This DoD directive refers to the 'Management and Control of Information Requirements'.

upvoted 3 times

Question #27 *Topic 1*

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.

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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.

Suggested Answer: *ABCDE*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

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

Suggested Answer: *BCDEF*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

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

A. Administrative

B. Technical

C. Power

D. Physical

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

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)

Suggested Answer: *A*

SusanGlenn5 1 year, 6 months ago

Never mind. I had to reread the question to understand it

upvoted 1 times

SusanGlenn5 1 year, 6 months ago

why not access control list...?

upvoted 1 times

Question #38 *Topic 1*

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

Suggested Answer: *B*

JTHOMAS1085 1 year, 5 months ago

Why are there so many Project Management questions in this CAP Exam?

upvoted 1 times

Question #39 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

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

Suggested Answer: *ABDE*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

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

Suggested Answer: *ABCDEG*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

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

Suggested Answer: *D*

Ramnik Highly Voted 1 year, 3 months ago

D is wrong Answer. Answer should A.

https://www.greycampus.com/opencampus/project-management-professional/plan-risk-responses
Outputs Of Monitor And Control Risks

The outputs are:

Risk register updates

Change requests, recommended preventive and corrective actions

Project management plan updates

Project document updates

Organizational process assets updates

upvoted 5 times

Question #53 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

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

A. OCTAVE

B. FITSAF

C. DITSCAP

D. FIPS 102

Suggested Answer: *D*

Ramnik 1 year, 3 months ago

https://flylib.com/books/en/1.564.1/understanding_certification_and_accreditation.html#fastmenu_8

FIPS 102 details a 6-step approach:

Planning
Data collection
Basic evaluation
Detailed evaluation
Report of findings
Accreditation

upvoted 3 times

Question #55 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

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

A. Phase 2

B. Phase 1

C. Phase 0

D. Phase 3

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

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

Suggested Answer: *ABEF*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

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

Suggested Answer: *D*

Ramnik 1 year, 3 months ago

It is now replaced by SP 800-115.

upvoted 3 times

Question #70 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

Which of the following objectives are defined by integrity in the C.I.A triad of information security systems?
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 modification of information by the unauthorized users.

D. It prevents the intentional or unintentional unauthorized disclosure of a message's contents .

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

Sam is the project manager of a construction project in south Florida. This area of the United
States is prone to hurricanes during certain parts of the year. As part of the project plan Sam and the project team acknowledge the possibility of hurricanes and the damage the hurricane could have on the project's deliverables, the schedule of the project, and the overall cost of the project. Once Sam and the project stakeholders acknowledge the risk of the hurricane they go on planning the project as if the risk is not likely to happen. What type of risk response is Sam using?

A. Mitigation

B. Avoidance

C. Passive acceptance

D. Active acceptance

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 1*

Fred is the project manager of the PKL project. He is working with his project team to complete the quantitative risk analysis process as a part of risk management planning. Fred understands that once the quantitative risk analysis process is complete, the process will need to be completed again in at least two other times in the project. When will the quantitative risk analysis process need to be repeated?

A. Quantitative risk analysis process will be completed again after the plan risk response planning and as part of procurement.

B. Quantitative risk analysis process will be completed again after the cost management planning and as a part of monitoring and controlling.

C. Quantitative risk analysis process will be completed again after new risks are identified and as part of monitoring and controlling.

D. Quantitative risk analysis process will be completed again after the risk response planning and as a part of monitoring and controlling.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

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

D. Avoid

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

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

Suggested Answer: *ABDE*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

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

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

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 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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

You are the project manager of the GHQ project for your company. You are working you're your project team to prepare for the qualitative risk analysis process.
Mary, a project team member, does not understand why you need to complete qualitative risks analysis. You explain to Mary that qualitative risks analysis helps you determine which risks needs additional analysis. There are also some other benefits that qualitative risks analysis can do for the project. Which one of the following is NOT an accomplishment of the qualitative risk analysis process?

A. Cost of the risk impact if the risk event occurs

B. Corresponding impact on project objectives

C. Time frame for a risk response

D. Prioritization of identified risk events based on probability and impact

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 1*

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. Discretionary Access Control

B. Mandatory Access Control

C. Policy Access Control

D. Role-Based Access Control

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

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

Suggested Answer: *ABCE*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 1*

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

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

Jeff, a key stakeholder in your project, wants to know how the risk exposure for the risk events is calculated during quantitative risk analysis. He is worried about the risk exposure which is too low for the events surrounding his project requirements. How is the risk exposure calculated?

A. The probability of a risk event plus the impact of a risk event determines the true risk expo sure.

B. The risk exposure of a risk event is determined by historical information.

C. The probability of a risk event times the impact of a risk event determines the true risk exposure.

D. The probability and impact of a risk event are gauged based on research and in-depth analysis.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 1*

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 Information System

C. Scope Verification

D. Integrated Change Control

Suggested Answer: *A*

rabbasi41 1 year ago

The Configuration Management System is a component of the change management system responsible for evaluating, testing, and documenting changes to the project scope and ensuring that these changes are systematically managed. It tracks and controls changes in project deliverables, including identifying which components are affected by the changes and ensuring they are properly documented and communicated.

upvoted 1 times

SusanGlenn5 1 year, 6 months ago

I'm pretty sure the answer is D

upvoted 2 times

Question #90 *Topic 1*

A project team member has just identified a new project risk. The risk event is determined to have significant impact but a low probability in the project. Should the risk event happen it'll cause the project to be delayed by three weeks, which will cause new risk in the project. What should the project manager do with the risk event?

A. Add the identified risk to a quality control management control chart.

B. Add the identified risk to the risk register.

C. Add the identified risk to the issues log.

D. Add the identified risk to the low-level risk watchlist.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

Which of the following concepts represent the three fundamental principles of information security?
Each correct answer represents a complete solution. Choose three.

A. Privacy

B. Integrity

C. Availability

D. Confidentiality

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

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

D. Business Unit Manager

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 1*

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

Suggested Answer: *ABCE*

CapTest 1 year, 6 months ago

The IAM/CA then makes certification accreditation recommendations to the DAA, and the DAA issues one of four accreditation determinations:

Approval to Operate (ATO) - Authorization of a DoD information system to process, store, or transmit information
Interim Approval to Operate (IATO) - Temporary approval to operate based on an assessment of the implementation status of the assigned IA Controls
Interim Approval to Test (IATT) - Temporary approval to conduct system testing based on an assessment of the implementation status of the assigned IA Controls
Denial of Approval to Operate (DATO) - A determination that a DoD information system cannot operate because of an inadequate IA design or failure to implement assigned IA Controls
upvoted 3 times

Question #95 *Topic 1*

Tom is the project manager for his organization. In his project he has recently finished the risk response planning. He tells his manager that he will now need to update the cost and schedule baselines. Why would the risk response planning cause Tom the need to update the cost and schedule baselines?

A. New or omitted work as part of a risk response can cause changes to the cost and/or schedule baseline.

B. Risk responses protect the time and investment of the project.

C. Baselines should not be updated, but refined through versions.

D. Risk responses may take time and money to implement.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

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. Risk rating

B. Warning signs

C. Cost of the project

D. Symptoms

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #97 *Topic 1*

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

Suggested Answer: *D*

Ramnik 1 year, 4 months ago
Looks to me answer is correct.

https://www.pm-primer.com/perform-quantitative-risk-analysis/
There is only one output from Quantitative risk analysis:

Risk register updates.

It is worth mentioning here are the risk is anything that may impact the objectives of a project, and this therefore must include positive and negative impacts. A negative impact risk is defined as a threat, and a positive impact risk is defined as an opportunity. Risk responses for threats should act two reduce the probability or impact, whereas risk response is for opportunities would want to maximize both the probability and impact should such a risk still occur.

With this in mind the risk register is updated as a result of Quantitative risk analysis in terms of its risk and probability along with the priority of each risk plus any trends that have been observed.
upvoted 3 times

Apprend7 1 year, 6 months ago
This one should be B
upvoted 1 times

skicat 2 years, 8 months ago
I thought a previous question stated it was QUALITATIVE that the output was risk register updates not quantitative
upvoted 2 times

Question #98 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 1*

Courtney is the project manager for her organization. She is working with the project team to complete the qualitative risk analysis for her project. During the analysis Courtney encourages the project team to begin the grouping of identified risks by common causes. What is the primary advantage to group risks by common causes during qualitative risk analysis?

A. It can lead to developing effective risk responses.

B. It can lead to the creation of risk categories unique to each project.

C. It helps the project team realize the areas of the project most laden with risks.

D. It saves time by collecting the related resources, such as project team members, to analyze the risk events.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #104 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #105 *Topic 1*

You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

A. Cost plus incentive fee

B. Time and materials

C. Cost plus percentage of costs

D. Fixed fee

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #106 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #107 *Topic 1*

You are the project manager of the GHY project for your organization. You are working with your project team to begin identifying risks for the project. As part of your preparation for identifying the risks within the project you will need eleven inputs for the process. Which one of the following is NOT an input to the risk identification process?

A. Cost management plan

B. Procurement management plan

C. Stakeholder register

D. Quality management plan

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #108 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #109 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #110 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #111 *Topic 1*

Thomas is the project manager of the NHJ Project for his company. He has identified several positive risk events within his project and he thinks these events can save the project time and money. Positive risk events, such as these within the NHJ Project are also known as what?

A. Opportunities

B. Benefits

C. Ancillary constituent components

D. Contingency risks

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #112 *Topic 1*

You are the project manager of the GGG project. You have completed the risk identification process for the initial phases of your project. As you begin to document the risk events in the risk register what additional information can you associate with the identified risk events?

A. Risk schedule

B. Risk potential responses

C. Risk cost

D. Risk owner

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #113 *Topic 1*

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.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #114 *Topic 1*

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

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #115 *Topic 1*

Mary is the project manager for the BLB project. She has instructed the project team to assemble, to review the risks. She has included the schedule management plan as an input for the quantitative risk analysis process. Why is the schedule management plan needed for quantitative risk analysis?

A. Mary will utilize the schedule controls and the nature of the schedule for the quantitative analysis of the schedule.

B. Mary will schedule when the identified risks are likely to happen and affect the project schedule.

C. Mary will utilize the schedule controls to determine how risks may be allowed to change the project schedule.

D. Mary will use the schedule management plan to schedule the risk identification meetings throughout the remaining project.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #116 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #117 *Topic 1*

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?

A. Phase 3

B. Phase 2

C. Phase 4

D. Phase 1

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #118 *Topic 1*

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?

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #119 *Topic 1*

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. Potential Risk Monitoring

B. Risk Management Planning

C. Quantitative Risk Analysis

D. Risk Monitoring and Control

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #120 *Topic 1*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #121 *Topic 1*

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

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #122 *Topic 1*

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. Penetration test

C. Paper test

D. Walk-through test

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #123 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #124 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #125 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #126 *Topic 1*

Which of the following statements is true about residual risks?

A. It is a weakness or lack of safeguard that can be exploited by a threat.

B. It can be considered as an indicator of threats coupled with vulnerability.

C. It is the probabilistic risk after implementing all security measures.

D. It is the probabilistic risk before implementing all security measures.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #127 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #128 *Topic 1*

You are the project manager of the GHY project for your organization. You are working with your project team to begin identifying risks for the project. As part of your preparation for identifying the risks within the project you will need eleven inputs for the process. Which one of the following is NOT an input to the risk identification process?

A. Cost management plan

B. Quality management plan

C. Procurement management plan

D. Stakeholder register

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #129 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #130 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #131 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #132 *Topic 1*

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

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #133 *Topic 1*

Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation?

A. Parkerian Hexad

B. Capability Maturity Model (CMM)

C. Classic information security model

D. Five Pillars model

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #134 *Topic 1*

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?

A. Teaming agreements

B. Crashing the project

C. Transference

D. Fast tracking the project

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #135 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #136 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #137 *Topic 1*

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. Continuity of Operations Plan

B. Disaster recovery plan

C. Contingency plan

D. Business continuity plan

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #138 *Topic 1*

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. System development

B. Certification analysis

C. Registration

D. Assessment of the Analysis Results

E. Configuring refinement of the SSAA

Suggested Answer: *ABDE*

Currently there are no comments in this discussion, be the first to comment!

Question #139 *Topic 1*

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

Suggested Answer: *ABCE*

Currently there are no comments in this discussion, be the first to comment!

Question #140 *Topic 1*

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 is the 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.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #141 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #142 *Topic 1*

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. Lack of consistency between the plans and the project requirements and assumptions can be the indicators of risk in the project.

B. The project documents will help the project manager, or Joan, to identify what risk identification approach is best to pursue.

C. Plans that have loose definitions of terms and disconnected approaches will reveal risks.

D. Poorly written requirements will reveal inconsistencies in the project plans and documents.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #143 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #144 *Topic 1*

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

Suggested Answer: *ACDEF*

Currently there are no comments in this discussion, be the first to comment!

Question #145 *Topic 1*

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 Response Plan

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #146 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #147 *Topic 1*

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. Quantitative analysis

B. Risk response plan

C. Contingency reserve

D. Risk response

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #148 *Topic 1*

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 process will analyze the effect of risk events that may substantially impact the project's competing demands.

B. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.

C. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.

D. 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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #149 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #150 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #151 *Topic 1*

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

A. Security plan

B. Security education

C. Security organization

D. Information classification

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #152 *Topic 1*

Which of the following is NOT a responsibility of a data owner?

A. Maintaining and protecting data

B. Ensuring that the necessary security controls are in place

C. Delegating responsibility of the day-to-day maintenance of the data protection mechanisms to the data custodian

D. Approving access requests

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #153 *Topic 1*

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 communications plan

B. Project management plan

C. Project contractual relationship with the vendor

D. Project scope statement

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #154 *Topic 1*

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

Suggested Answer: *ABDEFG*

Currently there are no comments in this discussion, be the first to comment!

Question #155 *Topic 1*

Harry is the project manager of the MMQ Construction Project. In this project Harry has identified a supplier who can create stained glass windows for 1,000 window units in the construction project. The supplier is an artist who works by himself, but creates windows for several companies throughout the United States.
Management reviews the proposal to use this supplier and while they agree that the supplier is talented, they do not think the artist can fulfill the 1,000 window units in time for the project's deadline. Management asked Harry to find a supplier who will guarantee the completion of the windows by the needed date in the schedule. What risk response has management asked Harry to implement?

A. Mitigation

B. Acceptance

C. Transference

D. Avoidance

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #156 *Topic 1*

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

A. PKI

B. Mutual authentication

C. Biometrics

D. Kerberos

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #157 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #158 *Topic 1*

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

B. Separation of duties

C. Need to Know

D. Due care

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #159 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #160 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #161 *Topic 1*

Which of the following formulas was developed by FIPS 199 for categorization of an information type?

A. SC information type = {(confidentiality, controls), (integrity, controls), (authentication, controls)}

B. SC information type = {(confidentiality, impact), (integrity, impact), (availability, impact)}

C. SC information type = {(confidentiality, risk), (integrity, risk), (availability, risk)}

D. SC information type = {(Authentication, impact), (integrity, impact), (availability, impact)}

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #162 *Topic 1*

Which of the following is NOT considered an environmental threat source?

A. Pollution

B. Hurricane

C. Chemical

D. Water

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #163 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #164 *Topic 1*

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)}

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #165 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #166 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #167 *Topic 1*

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

A. Initiation

B. Security certification

C. Operation

D. Maintenance

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #168 *Topic 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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #169 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #170 *Topic 1*

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

A. Phase 3

B. Phase 2

C. Phase 1

D. Phase 4

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #171 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #172 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #173 *Topic 1*

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

A. Testing

B. Examination

C. Interview

D. Debugging

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #174 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #175 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #176 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #177 *Topic 1*

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

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #178 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #179 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #180 *Topic 1*

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

D. RFP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #181 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #182 *Topic 1*

What approach can a project manager use to improve the project's performance during qualitative risk analysis?

A. Create a risk breakdown structure and delegate the risk analysis to the appropriate project team members.

B. Focus on high-priority risks.

C. Focus on near-term risks first.

D. Analyze as many risks as possible regardless of who initiated the risk event.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #183 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #184 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #185 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #186 *Topic 1*

Which of the following describes residual risk as the risk remaining after risk mitigation has occurred?

A. DIACAP

B. ISSO

C. SSAA

D. DAA

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #187 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #188 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #189 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #190 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #191 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #192 *Topic 1*

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 management plan

B. Project contractual relationship with the vendor

C. Project communications plan

D. Project scope statement

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #193 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #194 *Topic 1*

SIMULATION -

Fill in the blank with an appropriate word.

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

Suggested Answer: *Confidentiality*

Currently there are no comments in this discussion, be the first to comment!

Question #195 *Topic 1*

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 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 risk events have to pass the quantitative risk analysis process to develop effective risk responses.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #196 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #197 *Topic 1*

The Phase 4 of DITSCAP C&A is known as Post Accreditation. This phase starts after the system has been accredited in Phase 3. What are the process activities of this phase?
Each correct answer represents a complete solution. Choose all that apply.

A. Maintenance of the SSAA

B. Compliance validation

C. Change management

D. System operations

E. Security operations

F. Continue to review and refine the SSAA

Suggested Answer: *ABCDE*

Currently there are no comments in this discussion, be the first to comment!