Question #1 *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 are tested and reviewed

A. Level 4

B. Level 5

C. Level 1

D. Level 2

E. Level 3

Suggested Answer: *A*

Community vote distribution

A (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: A

Correct Answer. Level 4 is the "Tested and Reviewed Procedures and Controls" level.

upvoted 1 times

Cloud_Genius 5 years, 8 months ago

Ans. A is correct.

upvoted 3 times

Question #2 *Topic 1*

Which of the following is a type of security management for computers and networks in order to identify security breaches

A. IPS

B. IDS

C. ASA

D. EAP

Suggested Answer: *B*

ExamExam 1 year, 6 months ago

Identify -> Detect

IDS (B) is correct.

upvoted 3 times

Question #3 *Topic 1*

Which of the following types of firewalls increases the security of data packets by remembering the state of connection at the network and the session layers as they pass through the filter

A. Stateless packet filter firewall

B. PIX firewall

C. Stateful packet filter firewall

D. Virtual firewall

Suggested Answer: *C*

Community vote distribution

C (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: C

"A stateful firewall is a kind of firewall that keeps track and monitors the state of active network connections while analyzing incoming traffic and looking for potential traffic and data risks." from fortinet.com. The other firewalls are not capable, with the exception of possibly PIX, but not enough information about what model provided to be a concrete answer. C is the definitive answer.

upvoted 1 times

Question #4 *Topic 1*

Which of the following federal laws is designed to protect computer data from theft

A. Federal Information Security Management Act (FISMA)

B. Computer Fraud and Abuse Act (CFAA)

C. Government Information Security Reform Act (GISRA)

D. Computer Security Act

Suggested Answer: *B*

Community vote distribution

B (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: B

The remaining answers revolve around solutions for federal information systems.

upvoted 1 times

Question #5 *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. ATM

B. RTM

C. CRO

D. DAA

Suggested Answer: *B*

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

Question #6 *Topic 1*

Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one

A. Configuration Item Costing

B. Configuration Identification

C. Configuration Verification and Auditing

D. Configuration Status Accounting

Suggested Answer: *A*

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

Question #7 *Topic 1*

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

A. Authorizing Official

B. Information system owner

C. Chief Information Officer (CIO)

D. Chief Risk Officer (CRO)

Suggested Answer: *B*

Community vote distribution

B (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: B

Although the process is not exercised everywhere, according to ISSEP, the Sys Owner starts this process. Not sure I have ever run into a CRO before. Only the Sys Owner should be presenting their system for C&A.

upvoted 1 times

Question #8 *Topic 1*

Which of the following security controls is a set of layered security services that address communications and data security problems in the emerging Internet and intranet application space

A. Internet Protocol Security (IPSec)

B. Common data security architecture (CDSA)

C. File encryptors

D. Application program interface (API)

Suggested Answer: *B*

Community vote distribution

B (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: B

"The Common Data Security Architecture (CDSA) is a set of layered security services and cryptographic framework that provide an infrastructure for creating cross-platform, interoperable, security-enabled applications for client-server environments." - The OpenGroup. File encryptors is vague and doesn't make sense. An API is your programming space for a developer. IPSec is the IP Suite with Security.

upvoted 1 times

Question #9 *Topic 1*

Which of the following protocols is used to establish a secure terminal to a remote network device

A. WEP

B. SMTP

C. SSH

D. IPSec

Suggested Answer: *C*

Community vote distribution

C (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: C

SSH is used to remote into the CLI of most internetwork devices. SMTP is for mailing. WEP is an antiquated (but still used, unfortunately) WiFi protection solution. IPSec is the IP suite with security.

upvoted 1 times

Question #10 *Topic 1*

Which of the following elements of Registration task 4 defines the system's external interfaces as well as the purpose of each external interface, and the relationship between the interface and the system

A. System firmware

B. System software

C. System interface

D. System hardware

Suggested Answer: *C*

Community vote distribution

C (100%)

rebootitagain 1 year, 4 months ago

Selected Answer: C

That extremely long-worded question boils down to what provides a means of showing you how the hardware, software, and firmware interact with each other and allows you to make adjustments from one pane of glass. The only answer in this case would be the System Interface.

upvoted 1 times

Question #11 *Topic 1*

Which of the following guidelines is recommended for engineering, protecting, managing, processing, and controlling national security and sensitive (although unclassified) information

A. Federal Information Processing Standard (FIPS)

B. Special Publication (SP)

C. NISTIRs (Internal Reports)

D. DIACAP by the United States Department of Defense (DoD)

Suggested Answer: *B*

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

Question #12 *Topic 1*

Which of the following Security Control Assessment Tasks gathers the documentation and supporting materials essential for the assessment of the security controls in the information system

A. Security Control Assessment Task 4

B. Security Control Assessment Task 3

C. Security Control Assessment Task 1

D. Security Control Assessment Task 2

Suggested Answer: *C*

Community vote distribution

D (100%)

Bigboi2024 1 year, 4 months ago

Selected Answer: D

This task is where the actual collection of evidence and documentation usually takes place. The assessors would gather all the necessary materials, such as policies, procedures, system configurations, and audit logs, to evaluate the security controls in the information system.

upvoted 1 times

Ewetayo 1 year, 9 months ago

D. Security Control Assessment Task 2: Reviewing security control documentation and supporting materials, which involves gathering the necessary documentation and materials needed to assess the security controls.

upvoted 2 times

Question #13 *Topic 1*

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

A. Chief Information Officer

B. Authorizing Official

C. Common Control Provider

D. Senior Agency Information Security Officer

Suggested Answer: *C*

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

Question #14 *Topic 1*

Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls

A. Certification and accreditation (C&A)

B. Risk Management

C. Information systems security engineering (ISSE)

D. Information Assurance (IA)

Suggested Answer: *A*

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

Question #15 *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. Security operations

B. Continue to review and refine the SSAA

C. Change management

D. Compliance validation

E. System operations

F. Maintenance of the SSAA

Suggested Answer: *EAFCD*

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

Question #16 *Topic 1*

Which of the following email lists is written for the technical audiences, and provides weekly summaries of security issues, new vulnerabilities, potential impact, patches and workarounds, as well as the actions recommended to mitigate risk

A. Cyber Security Tip

B. Cyber Security Alert

C. Cyber Security Bulletin

D. Technical Cyber Security Alert

Suggested Answer: *C*

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

Question #17 *Topic 1*

Which of the following tasks obtains the customer agreement in planning the technical effort

A. Task 9

B. Task 11

C. Task 8

D. Task 10

Suggested Answer: *B*

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

Question #18 *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 800-59

B. NIST Special Publication 800-60

C. NIST Special Publication 800-37A

D. NIST Special Publication 800-37

E. NIST Special Publication 800-53

F. NIST Special Publication 800-53A

Suggested Answer: *DEFAB*

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

Question #19 *Topic 1*

Which of the following elements are described by the functional requirements task Each correct answer represents a complete solution. Choose all that apply.

A. Coverage

B. Accuracy

C. Quality

D. Quantity

Suggested Answer: *DCA*

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

Question #20 *Topic 1*

Which of the following documents is defined as a source document, which is most useful for the ISSE when classifying the needed security functionality

A. Information Protection Policy (IPP)

B. IMM

C. System Security Context

D. CONOPS

Suggested Answer: *A*

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

Question #21 *Topic 1*

DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires basic integrity and availability

A. MAC I

B. MAC II

C. MAC IV

D. MAC III

Suggested Answer: *D*

rebootitagain 1 year, 4 months ago

MAC 2 requires high integrity and medium availability. MAC 1 requires both high integrity and availability. MAC 4 does not exist to the best of my knowledge. Good outlier, though.

upvoted 1 times

Question #22 *Topic 1*

What are the responsibilities of a system owner Each correct answer represents a complete solution. Choose all that apply.

A. Integrates security considerations into application and system purchasing decisions and development projects.

B. Ensures that the necessary security controls are in place.

C. Ensures that adequate security is being provided by the necessary controls, password management, remote access controls, operating system configurations, and so on.

D. Ensures that the systems are properly assessed for vulnerabilities and must report any to the incident response team and data owner.

Suggested Answer: *CDA*

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

Question #23 *Topic 1*

Which of the following Registration Tasks sets up the business or operational functional description and system identification

A. Registration Task 2

B. Registration Task 1

C. Registration Task 3

D. Registration Task 4

Suggested Answer: *B*

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

Question #24 *Topic 1*

SIMULATION -

Fill in the blank with an appropriate section name. _____ is a section of the SEMP template, which specifies the methods and reasoning planned to build the requisite trade-offs between functionality, performance, cost, and risk.

Suggested Answer: *System Analysis*

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

Question #25 *Topic 1*

Which of the following federal agencies provides a forum for the discussion of policy issues, sets national policy, and promulgates direction, operational procedures, and guidance for the security of national security systems

A. National Security AgencyCentral Security Service (NSACSS)

B. National Institute of Standards and Technology (NIST)

C. United States Congress

D. Committee on National Security Systems (CNSS)

Suggested Answer: *D*

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

Question #26 *Topic 1*

Which of the following statements is true about residual risks

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

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

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 #27 *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. EC Enclave and Computing Environment

C. VI Vulnerability and Incident Management

D. Information systems acquisition, development, and maintenance

Suggested Answer: *ACB*

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

Question #28 *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 a comprehensive assessment of the management, operational, and technical security controls in an information system.

B. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.

C. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.

D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

Suggested Answer: *CB*

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

Question #29 *Topic 1*

Which of the following protocols is built in the Web server and browser to encrypt data traveling over the Internet

A. UDP

B. SSL

C. IPSec

D. HTTP

Suggested Answer: *B*

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

Question #30 *Topic 1*

Which of the following configuration management system processes defines which items will be configuration managed, how they are to be identified, and how they are to be documented

A. Configuration verification and audit

B. Configuration control

C. Configuration status accounting

D. Configuration identification

Suggested Answer: *D*

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

Question #31 *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. Initiate IA implementation plan.

C. Conduct validation activity.

D. Assemble DIACAP team.

E. Register system with DoD Component IA Program.

F. Assign IA controls.

Suggested Answer: *EFDAB*

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

Question #32 *Topic 1*

You work as a security engineer for BlueWell Inc. Which of the following documents will you use as a guide for the security certification and accreditation of

Federal Information Systems -

A. NIST Special Publication 800-59

B. NIST Special Publication 800-37

C. NIST Special Publication 800-60

D. NIST Special Publication 800-53

Suggested Answer: *B*

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

Question #33 *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 management plan

B. Project charter

C. Quality management plan

D. Risk register

Suggested Answer: *D*

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

Question #34 *Topic 1*

Diane is the project manager of the HGF Project. A risk that has been identified and analyzed in the project planning processes is now coming into fruition. What individual should respond to the risk with the preplanned risk response

A. Project sponsor

B. Risk owner

C. Diane

D. Subject matter expert

Suggested Answer: *B*

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

Question #35 *Topic 1*

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

A. Classic information security model

B. Certification and Accreditation (C&A)

C. Information Assurance (IA)

D. Five Pillars model

Suggested Answer: *B*

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

Question #36 *Topic 1*

In which of the following phases of the interconnection life cycle as defined by NIST SP 800-47, do the organizations build and execute a plan for establishing the interconnection, including executing or configuring appropriate security controls

A. Establishing the interconnection

B. Planning the interconnection

C. Disconnecting the interconnection

D. Maintaining the interconnection

Suggested Answer: *A*

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

Question #37 *Topic 1*

Which of the following tools demands involvement by upper executives, in order to integrate quality into the business system and avoid delegation of quality functions to junior administrators

A. ISO 90012000

B. Benchmarking

C. SEI-CMM

D. Six Sigma

Suggested Answer: *A*

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

Question #38 *Topic 1*

Which of the following documents contains the threats to the information management, and the security services and controls required to counter those threats

A. System Security Context

B. Information Protection Policy (IPP)

C. CONOPS

D. IMM

Suggested Answer: *B*

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

Question #39 *Topic 1*

Which of the following statements define the role of the ISSEP during the development of the detailed security design, as mentioned in the IATF document Each correct answer represents a complete solution. Choose all that apply.

A. It identifies the information protection problems that needs to be solved.

B. It allocates security mechanisms to system security design elements.

C. It identifies custom security products.

D. It identifies candidate commercial off-the-shelf (COTS)government off-the-shelf (GOTS) security products.

Suggested Answer: *BDC*

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

Question #40 *Topic 1*

Which of the following individuals is responsible for the oversight of a program that is supported by a team of people that consists of, or be exclusively comprised of contractors

A. Quality Assurance Manager

B. Senior Analyst

C. System Owner

D. Federal program manager

Suggested Answer: *D*

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

Question #41 *Topic 1*

Which of the following agencies serves the DoD community as the largest central resource for DoD and government-funded scientific, technical, engineering, and business related information available today

A. DISA

B. DIAP

C. DTIC

D. DARPA

Suggested Answer: *C*

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

Question #42 *Topic 1*

You work as a system engineer for BlueWell Inc. You want to verify that the build meets its data requirements, and correctly generates each expected display and report. Which of the following tests will help you to perform the above task

A. Functional test

B. Reliability test

C. Performance test

D. Regression test

Suggested Answer: *A*

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

Question #43 *Topic 1*

You work as a system engineer for BlueWell Inc. Which of the following documents will help you to describe the detailed plans, procedures, and schedules to guide the transition process

A. Configuration management plan

B. Transition plan

C. Systems engineering management plan (SEMP)

D. Acquisition plan

Suggested Answer: *B*

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

Question #44 *Topic 1*

Which of the following policies describes the national policy on the secure electronic messaging service

A. NSTISSP No. 11

B. NSTISSP No. 7

C. NSTISSP No. 6

D. NSTISSP No. 101

Suggested Answer: *B*

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

Question #45 *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. Computer Misuse Act

B. Clinger-Cohen Act

C. ISG

D. Lanham Act

Suggested Answer: *C*

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

Question #46 *Topic 1*

Which of the following principles are defined by the IATF model Each correct answer represents a complete solution. Choose all that apply.

A. The degree to which the security of the system, as it is defined, designed, and implemented, meets the security needs.

B. The problem space is defined by the customer's mission or business needs.

C. The systems engineer and information systems security engineer define the solution space, which is driven by the problem space.

D. Always keep the problem and solution spaces separate.

Suggested Answer: *DBC*

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

Question #47 *Topic 1*

Which of the following cooperative programs carried out by NIST conducts research to advance the nation's technology infrastructure

A. Manufacturing Extension Partnership

B. NIST Laboratories

C. Baldrige National Quality Program

D. Advanced Technology Program

Suggested Answer: *B*

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

Question #48 *Topic 1*

Which of the following persons in an organization is responsible for rejecting or accepting the residual risk for a system

A. System Owner

B. Information Systems Security Officer (ISSO)

C. Designated Approving Authority (DAA)

D. Chief Information Security Officer (CISO)

Suggested Answer: *C*

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

Question #49 *Topic 1*

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

A. FITSAF

B. OCTAVE

C. FIPS 102

D. DITSCAP

Suggested Answer: *C*

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

Question #50 *Topic 1*

What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process Each correct answer represents a complete solution. Choose all that apply.

A. Conduct activities related to the disposition of the system data and objects.

B. Combine validation results in DIACAP scorecard.

C. Conduct validation activities.

D. Execute and update IA implementation plan.

Suggested Answer: *DCB*

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

Question #51 *Topic 1*

Which of the following memorandums reminds the Federal agencies that it is required by law and policy to establish clear privacy policies for Web activities and to comply with those policies

A. OMB M-01-08

B. OMB M-03-19

C. OMB M-00-07

D. OMB M-00-13

Suggested Answer: *D*

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

Question #52 *Topic 1*

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

A. The level of detail must define exactly the risk response for each identified risk.

B. The level of detail is set of project risk governance.

C. The level of detail is set by historical information.

D. The level of detail should correspond with the priority ranking.

Suggested Answer: *D*

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

Question #53 *Topic 1*

You work as a security manager for BlueWell Inc. You are going through the NIST SP 800-37 C&A methodology, which is based on four well defined phases. In which of the following phases of NIST SP 800-37 C&A methodology does the security categorization occur

A. Continuous Monitoring

B. Initiation

C. Security Certification

D. Security Accreditation

Suggested Answer: *B*

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

Question #54 *Topic 1*

You work as a systems engineer for BlueWell Inc. You are working on translating system requirements into detailed function criteria. Which of the following diagrams will help you to show all of the function requirements and their groupings in one diagram

A. Activity diagram

B. Functional flow block diagram (FFBD)

C. Functional hierarchy diagram

D. Timeline analysis diagram

Suggested Answer: *C*

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

Question #55 *Topic 1*

Which of the following phases of DITSCAP includes the activities that are necessary for the continuing operation of an accredited IT system in its computing environment and for addressing the changing threats that a system faces throughout its life cycle

A. Phase 1, Definition

B. Phase 3, Validation

C. Phase 4, Post Accreditation Phase

D. Phase 2, Verification

Suggested Answer: *C*

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

Question #56 *Topic 1*

Which of the following Security Control Assessment Tasks evaluates the operational, technical, and the management security controls of the information system using the techniques and measures selected or developed

A. Security Control Assessment Task 3

B. Security Control Assessment Task 1

C. Security Control Assessment Task 4

D. Security Control Assessment Task 2

Suggested Answer: *A*

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

Question #57 *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. Assessment of the Analysis Results

B. Certification analysis

C. Registration

D. System development

E. Configuring refinement of the SSAA

Suggested Answer: *EDBA*

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

Question #58 *Topic 1*

You work as a Network Administrator for PassGuide Inc. You need to secure web services of your company in order to have secure transactions. Which of the following will you recommend for providing security

A. HTTP

B. VPN

C. SMIME

D. SSL

Suggested Answer: *D*

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

Question #59 *Topic 1*

Which of the following processes illustrate the study of a technical nature of interest to focused audience, and consist of interim or final reports on work made by
NIST for external sponsors, including government and non-government sponsors

A. Federal Information Processing Standards (FIPS)

B. Special Publication (SP)

C. NISTIRs (Internal Reports)

D. DIACAP

Suggested Answer: *C*

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

Question #60 *Topic 1*

SIMULATION -

Fill in the blank with an appropriate phrase. _____ seeks to improve the quality of process outputs by identifying and removing the causes of defects and variability in manufacturing and business processes.

Suggested Answer: *Six Sigma*

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

Question #61 *Topic 1*

You work as a security engineer for BlueWell Inc. You are working on the ISSE model. In which of the following phases of the ISSE model is the system defined in terms of what security is needed

A. Define system security architecture

B. Develop detailed security design

C. Discover information protection needs

D. Define system security requirements

Suggested Answer: *D*

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

Question #62 *Topic 1*

TQM recognizes that quality of all the processes within an organization contribute to the quality of the product. Which of the following are the most important activities in the Total Quality Management Each correct answer represents a complete solution. Choose all that apply.

A. Quality renewal

B. Maintenance of quality

C. Quality costs

D. Quality improvements

Suggested Answer: *BDA*

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

Question #63 *Topic 1*

SIMULATION -

Fill in the blank with the appropriate phrase. The _____ is the risk that remains after the implementation of new or enhanced controls.

Suggested Answer: *residual risk*

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

Question #64 *Topic 1*

Which of the following is designed to detect unwanted attempts at accessing, manipulating, and disabling of computer systems through the Internet

A. DAS

B. IDS

C. ACL

D. Ipsec

Suggested Answer: *B*

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

Question #65 *Topic 1*

Which of the following security controls is standardized by the Internet Engineering Task Force (IETF) as the primary network layer protection mechanism

A. Internet Key Exchange (IKE) Protocol

B. SMIME

C. Internet Protocol Security (IPSec)

D. Secure Socket Layer (SSL)

Suggested Answer: *C*

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

Question #66 *Topic 1*

Which of the following DoD policies provides assistance on how to implement policy, assign responsibilities, and prescribe procedures for applying integrated, layered protection of the DoD information systems and networks

A. DoD 8500.1 Information Assurance (IA)

B. DoDI 5200.40

C. DoD 8510.1-M DITSCAP

D. DoD 8500.2 Information Assurance Implementation

Suggested Answer: *D*

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

Question #67 *Topic 1*

Which of the following is a document, usually in the form of a table, that correlates any two baseline documents that require a many-to-many relationship to determine the completeness of the relationship

A. FIPS 200

B. NIST SP 800-50

C. Traceability matrix

D. FIPS 199

Suggested Answer: *C*

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

Question #68 *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 manages the security of the information system that is slated for Certification & Accreditation (C&A).

B. An ISSE provides advice on the impacts of system changes.

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

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

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

Suggested Answer: *DBC*

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

Question #69 *Topic 1*

SIMULATION -

For interactive and self-paced preparation of exam ISSEP, try our practice exams.

Practice exams also include self assessment and reporting features!

Fill in the blank with an appropriate word. _____ has the goal to securely interconnect people and systems independent of time or location.

Suggested Answer: *Netcentric*

usako 1 year, 2 months ago

This seems to be a sample question from another training provider.

upvoted 1 times

Question #70 *Topic 1*

Which of the following configuration management system processes keeps track of the changes so that the latest acceptable configuration specifications are readily available

A. Configuration Identification

B. Configuration Verification and Audit

C. Configuration Status and Accounting

D. Configuration Control

Suggested Answer: *C*

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

Question #71 *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. FITSAF

C. FIPS

D. TCSEC

Suggested Answer: *A*

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

Question #72 *Topic 1*

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using

A. Risk acceptance

B. Risk mitigation

C. Risk avoidance

D. Risk transfer

Suggested Answer: *D*

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

Question #73 *Topic 1*

Which of the following responsibilities are executed by the federal program manager

A. Ensure justification of expenditures and investment in systems engineering activities.

B. Coordinate activities to obtain funding.

C. Review project deliverables.

D. Review and approve project plans.

Suggested Answer: *ABD*

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

Question #74 *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. Right-Up Approach

B. Left-Up Approach

C. Bottom-Up Approach

D. Top-Down Approach

Suggested Answer: *DC*

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

Question #75 *Topic 1*

SIMULATION -

Fill in the blank with the appropriate phrase. _____ provides instructions and directions for completing the Systems Security Authorization Agreement

(SSAA).

Suggested Answer: *DoDI 5200.40*

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

Question #76 *Topic 1*

Which of the following acts promote a risk-based policy for cost effective security Each correct answer represents a part of the solution. Choose all that apply.

A. Clinger-Cohen Act

B. Lanham Act

C. Paperwork Reduction Act (PRA)

D. Computer Misuse Act

Suggested Answer: *CA*

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

Question #77 *Topic 1*

Which of the following tasks prepares the technical management plan in planning the technical effort

A. Task 10

B. Task 9

C. Task 7

D. Task 8

Suggested Answer: *B*

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

Question #78 *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 800-37

C. NIST SP 800-59

D. NIST SP 800-42

E. NIST SP 800-53A

F. NIST SP 800-53

Suggested Answer: *D*

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

Question #79 *Topic 1*

Which of the following Registration Tasks sets up the system architecture description, and describes the C&A boundary

A. Registration Task 3

B. Registration Task 4

C. Registration Task 2

D. Registration Task 1

Suggested Answer: *B*

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

Question #80 *Topic 1*

Stella works as a system engineer for BlueWell Inc. She wants to identify the performance thresholds of each build. Which of the following tests will help Stella to achieve her task

A. Regression test

B. Reliability test

C. Functional test

D. Performance test

Suggested Answer: *D*

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

Question #81 *Topic 1*

Which of the following cooperative programs carried out by NIST encourages performance excellence among U.S. manufacturers, service companies, educational institutions, and healthcare providers

A. Manufacturing Extension Partnership

B. Baldrige National Quality Program

C. Advanced Technology Program

D. NIST Laboratories

Suggested Answer: *B*

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

Question #82 *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 profit. If your organization seizes this opportunity it would be an example of what risk response

A. Enhancing

B. Positive

C. Opportunistic

D. Exploiting

Suggested Answer: *D*

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

Question #83 *Topic 1*

Which of the following processes provides guidance to the system designers and form the basis of major events in the acquisition phases, such as testing the products for system integration

A. Operational scenarios

B. Functional requirements

C. Human factors

D. Performance requirements

Suggested Answer: *A*

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

Question #84 *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. Which of the following participants are required in a NIACAP security assessment? Each correct answer represents a part of the solution. Choose all that apply.

A. Information Assurance Manager

B. Designated Approving Authority

C. Certification agent

D. IS program manager

E. User representative

Suggested Answer: *BCDE*

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

Question #85 *Topic 1*

Which of the following is NOT used in the practice of Information Assurance (IA) to define assurance requirements

A. Classic information security model

B. Five Pillars model

C. Communications Management Plan

D. Parkerian Hexad

Suggested Answer: *C*

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

Question #86 *Topic 1*

Which of the following NIST documents describes that minimizing negative impact on an organization and a need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems

A. NIST SP 800-37

B. NIST SP 800-30

C. NIST SP 800-53

D. NIST SP 800-60

Suggested Answer: *B*

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

Question #87 *Topic 1*

Which of the following roles is also known as the accreditor

A. Data owner

B. Chief Information Officer

C. Chief Risk Officer

D. Designated Approving Authority

Suggested Answer: *D*

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

Question #88 *Topic 1*

In which of the following DIACAP phases is residual risk analyzed

A. Phase 2

B. Phase 3

C. Phase 5

D. Phase 1

E. Phase 4

Suggested Answer: *E*

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

Question #89 *Topic 1*

Which of the following CNSS policies describes the national policy on controlled access protection

A. NSTISSP No. 101

B. NSTISSP No. 200

C. NCSC No. 5

D. CNSSP No. 14

Suggested Answer: *B*

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

Question #90 *Topic 1*

Which of the following agencies is responsible for funding the development of many technologies such as computer networking, as well as NLS

A. DARPA

B. DTIC

C. DISA

D. DIAP

Suggested Answer: *A*

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

Question #91 *Topic 1*

Which of the following organizations is a USG initiative designed to meet the security testing, evaluation, and assessment needs of both information technology
(IT) producers and consumers

A. NSA

B. NIST

C. CNSS

D. NIAP

Suggested Answer: *D*

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

Question #92 *Topic 1*

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

A. Warranties

B. Performance bonds

C. Use of insurance

D. Life cycle costing

Suggested Answer: *D*

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

Question #93 *Topic 1*

You work as a security engineer for BlueWell Inc. According to you, which of the following DITSCAPNIACAP model phases occurs at the initiation of the project, or at the initial C&A effort of a legacy system

A. Post Accreditation

B. Definition

C. Verification

D. Validation

Suggested Answer: *B*

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

Question #94 *Topic 1*

SIMULATION -

Fill in the blank with an appropriate phrase. A _____ is defined as any activity that has an effect on defining, designing, building, or executing a task, requirement, or procedure.

Suggested Answer: *technical effort*

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

Question #95 *Topic 1*

According to which of the following DoD policies, the implementation of DITSCAP is mandatory for all the systems that process both DoD classified and unclassified information?

A. DoD 8500.2

B. DoDI 5200.40

C. DoD 8510.1-M DITSCAP

D. DoD 8500.1 (IAW)

Suggested Answer: *D*

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

Question #96 *Topic 1*

Which of the following federal laws are related to hacking activities Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030

B. 18 U.S.C. 1029

C. 18 U.S.C. 2510

D. 18 U.S.C. 1028

Suggested Answer: *CBA*

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

Question #97 *Topic 1*

Which of the following Registration Tasks notifies the DAA, Certifier, and User Representative that the system requires C&A Support

A. Registration Task 4

B. Registration Task 1

C. Registration Task 3

D. Registration Task 2

Suggested Answer: *D*

usako 1 year, 2 months ago

The answer should be B, according to the DITSCAP...

upvoted 1 times

Question #98 *Topic 1*

Which of the following are the most important tasks of the Information Management Plan (IMP) Each correct answer represents a complete solution. Choose all that apply.

A. Define the Information Protection Policy (IPP).

B. Define the System Security Requirements.

C. Define the mission need.

D. Identify how the organization manages its information.

Suggested Answer: *CDA*

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

Question #99 *Topic 1*

FIPS 199 defines the three levels of potential impact on organizations. Which of the following potential impact levels shows limited adverse effects on organizational operations, organizational assets, or individuals

A. Moderate

B. Medium

C. High

D. Low

Suggested Answer: *D*

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

Question #100 *Topic 1*

The principle of the SEMP is not to repeat the information, but rather to ensure that there are processes in place to conduct those functions. Which of the following sections of the SEMP template describes the work authorization procedures as well as change management approval processes

A. Section 3.1.8

B. Section 3.1.9

C. Section 3.1.5

D. Section 3.1.7

Suggested Answer: *B*

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

Question #101 *Topic 1*

Which of the of following departments protects and supports DoD information, information systems, and information networks that are critical to the department and the armed forces during the day-to-day operations, and in the time of crisis

A. DIAP

B. DARPA

C. DTIC

D. DISA

Suggested Answer: *A*

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

Question #102 *Topic 1*

Which of the following organizations incorporates building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions

A. DTIC

B. NSA IAD

C. DIAP

D. DARPA

Suggested Answer: *B*

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

Question #103 *Topic 1*

Which of the following federal laws establishes roles and responsibilities for information security, risk management, testing, and training, and authorizes NIST and
NSA to provide guidance for security planning and implementation

A. Computer Fraud and Abuse Act

B. Government Information Security Reform Act (GISRA)

C. Federal Information Security Management Act (FISMA)

D. Computer Security Act

Suggested Answer: *B*

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

Question #104 *Topic 1*

Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system

A. Phase 3

B. Phase 2

C. Phase 4

D. Phase 1

Suggested Answer: *B*

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

Question #105 *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. SSAA

B. TCSEC

C. FIPS

D. FITSAF

Suggested Answer: *B*

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

Question #106 *Topic 1*

What NIACAP certification levels are recommended by the certifier Each correct answer represents a complete solution. Choose all that apply.

A. Basic System Review

B. Basic Security Review

C. Maximum Analysis

D. Comprehensive Analysis

E. Detailed Analysis

F. Minimum Analysis

Suggested Answer: *BFED*

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

Question #107 *Topic 1*

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

A. Abbreviated

B. Significant

C. Substantial

D. Comprehensive

Suggested Answer: *A*

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